NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

WHO NETWORKS? THE SOCIAL PSYCHOLOGY OF VIRTUAL COMMUNITIES

by

James B. Kinniburgh

June 2004

Thesis Advisor:	Dorothy Denning
Second Reader:	John Arquilla

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for information operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Who Networks? The Social Psychology of Virtual Communities		**5. FUNDING NUMBERS**	
6. AUTHOR(S) James B. Kinniburgh			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words) SOF members must be fully capable (fluent and adept) at operating in, through and upon networks to maximize the leverage of information technologies. Military information operators must possess the components of network capital (access to technology, computer literacy, and social networking ability), a strong tendency to engage in trusting behavior, high cognitive ability and a formal education. Virtual communities offer a mosaic of social behaviors and practices that provide models for virtual organization(s) within the military. Computer-mediated communications technologies (CMCTs) provide an inherently neutral but polymorphic forum for human social interaction (cyberspace). Specific emergent social topology (real or virtual) depends on the local social needs of individuals and/or bounded groups (communities). Because differences in topology are emergent, topological models have little predictive value. Virtual communities are better understood and predicted through analysis of their metadata. Virtual communities can be characterized as open or clandestine, according to their purpose, accessibility, level of trust, and primary *mode* of connectedness (bonding or bridging ties). Both open and clandestine communities offer methods of ensuring high levels of efficiency, trust, and security within military computer-mediated communications networks, as well as providing models of organizational flexibility that can be adapted to SOF missions and roles.

14. SUBJECT TERMS Computers, Networks, Virtual Communities, Sociology, Cybersociology, Netwar, Information Operations, Information Warfare, Psychology, Society, Intelligence, Special Operations, Communications.			**15. NUMBER OF PAGES** 148
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

WHO NETWORKS? THE SOCIAL PSYCHOLOGY OF VIRTUAL COMMUNITIES

James B. Kinniburgh
Captain, United States Air Force
B.A., University of Oklahoma, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
June 2004

Author: James B. Kinniburgh

Approved by: Dr. Dorothy Denning
Thesis Advisor

Dr. John Arquilla
Second Reader/Co-Advisor

Dr. Gordon McCormick
Chairman, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis explores recent thinking regarding the organizational restructuring of special operations forces (SOF) to optimize their use of advances in information technologies in the global war on terrorism (GWOT). These ideas have implied the need to push decisional authority away from the center and to distribute it among regionally diverse teams, based on the proposition that because the new generation of terrorists seems to operate in flat, open-ended associations, we must mirror their strategy. To do this, SOF members must be able, among other things, to maximize the advantages afforded by information technologies. They must be fully capable (fluent and adept) at operating in, through and upon networks.

Networkers, the "digerati," or in the case of the military, *netwarriors* must possess the components of *network capital* (access to technology, computer literacy, and social networking ability), a strong tendency to engage in *trusting behavior*, high *cognitive ability* and some *education*. These qualities are useful in not only specialized information warriors, but also all across a highly networked military in general. Virtual communities (i.e., societies that form and exist mostly in cyberspace) offer a mosaic of social behaviors and practices that may provide models for virtual organization(s) within the military

Computer-mediated communications technologies (CMCTs) provide an inherently neutral but polymorphic forum for human social interaction (cyberspace). Specific emergent social topology (real or virtual) depends on the *local* social needs of individuals and/or bounded groups (communities). Because differences in topology are emergent, topological models have little predictive value. Virtual communities are better understood and predicted through an analysis of their *metadata*. Virtual communities can best be characterized as *open* or *clandestine*, according to their *purpose*, *accessibility*, level of *trust*, and primary *mode of connectedness* (bonding or bridging ties).

Both open and clandestine communities offer methods of ensuring high levels of efficiency, trust, and security within military computer-mediated communications networks, as well as providing models of organizational flexibility that can be adapted to SOF missions and roles.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Senior Special Agent James Clemente, Behavioral Analysis Unit, FBI HQ

Special Agent Kristen Sheldon, Computer Crimes Division, FBI Houston, TX

Special Agent Ron Yearwood, Computer Crimes Division, FBI Houston, TX

Special Agent Chuck St Pierre, AFOSI, Monterey, CA

Dr. Al Cooper, Director, San Jose Marital and Sexuality Center, San Jose, CA

Dr./Major Nate Galbraith, Andrews AFB

Detective James McLaughlin, City of Keene Police Department, NH

Dr. Glenn Robinson, Professor of Middle Eastern Studies, NPS

Dr. Anna Simons, Professor of Anthropology, NPS

Dr. Eric Jansen, Professor of Organizational Studies, NPS

Michael Knapp, Asymmetric Warfare Analyst, Africa/Middle East Division, National Ground Intelligence Center

Sony Online Entertainment and Verant Interactive

AOL/Time-Warner

Various *EverQuest*ors and AOL chat participants

I. INTRODUCTION

A. PURPOSE

The purpose of this study is to examine the behaviors of individuals who network extensively, particularly those who tend to live a significant portion of their lives on-line, to discover whether there are skills (social and technical), aptitudes, attitudes, and modes of thought particular to intensive networkers. This study will also examine the types of virtual communities in which these individuals participate, with an emphasis on observing and explaining any emergent architecture, patterns of behavior and membership in such communities.

B. AREA OF RESEARCH

The USAF Institute for National Security Studies (INSS) has noted that advances in technology are redefining national security and military operations. Recognizing that successful information operations may require an entirely different set of aptitudes and skills, the INSS put out a call for research into various areas, including the question, "How can you build (assess and train) an information warfare (IW) capable force?"

The unspoken, but understood implication here is that IW means primarily computer network attack (CNA), computer network exploitation (CNE) and computer network defense (CND), as opposed to other areas of IW such as electronic warfare (EW), psychological operations (PSYOP), and military deception. However, as the entire force has adopted the use of computer networks, the necessity for online skills has expanded beyond the narrow purview of CNA/D/E. Organizational structures, effective leadership and management, C2, intelligence collection, analysis and dissemination, peer relationships, coordination of and among distributed teams and/or groups online, and establishing relationships with foreign counterparts or civilians have all been affected by the ubiquity and utility of military computer networks. Does this shift in the way members communicate and relate imply necessary changes in the way military services and units organize, in the people we seek to recruit, in the way we reward and promote them?

As the United States Armed Forces seek to develop and expand their human information operations capabilities to exploit the possibilities of cyberspace, specific questions of military importance include the following identified by the INSS:

- Is there any effective way to recruit the "info operators" necessary to maintain superiority in the various aspects of information warfare operations?
- Are we currently using effective techniques for recruiting airmen, soldiers, and sailors who are better suited to information operations?
- Do entrance tests (enlisted or officer) adequately measure the aptitude and skills needed for IW?
- Should recruiting of IW be tailored differently than other military fields?

However, identifying the characteristics of people who work well online has broader implications than just finding good information warriors. Indeed, most military use of cyberspace is not IW per se. In the Air Force, for example, the information management career field and the community of air intelligence analysts and collectors need to be completely fluent in using and perhaps even configuring the new technologies that facilitate pooling, sharing and fusing information. Special operations forces (SOF) offer another example: Recent suggestions regarding the restructuring of special operations forces (SOF) to better exploit information technologies in the global war on terrorism (GWOT) have emphasized the necessity of pushing decisional authority away from the center and distributing it among regionally diverse teams, on the proposition that because the new generation of terrorists seems to operate in flat, open ended associations, we must mirror their strategy. SOF members must be prepared to be able to maximize the leverage of information technologies. They must be fully capable (fluent and adept) at operating in, through and upon networks.

New network mapping/influence modeling and visualization software can provide effective targeting tools for information operations by providing a cognitive framework for assembling and understanding the multilayered *metadata* which constitute the rules underlying network behavior, and which become the instrumentalities and objects of manipulation in information operations. Certain architectures used in peer-to-peer (p2p) networks can facilitate distributed, adaptive military intelligence and communications

networks while maintaining the personal accountability so crucial to trust in both the intelligence and Special Operations communities. An examination of these technologies is inseparable from an examination of the people and communities who use them.

C. RESEARCH QUESTIONS

1. Primary Research Question

Who networks? What individual skill sets, aptitudes, preferences and behaviors should the military seek to recruit, reward and promote to maintain superiority in the various aspects of information warfare and computer network operations fundamental to all combat and support activities?

2. Subsidiary Research Questions

1. What defines a virtual community? Do differences in virtual forums constitute differences in communities? What broad distinctions can we make among various virtual communities?
2. What factors, such as wealth or availability of Internet access, might lead and enable a person to participate in virtual communities?
3. What do online communities offer their members to induce them to participate; i.e., what is the “reward structure”?
4. What general patterns of behavior emerge among those who network?
5. Do their social and/or cognitive skill sets differ from those of the population at large?
6. Some people may have very good computer network skills, but do not actively participate in online communities as "speakers". They might rather just "listen", e.g., by signing up for e-mail distribution lists, reading message boards, or “lurking” in chat rooms. Does it matter if one is a speaker or listener? What about those who show leadership in online communities?

D. SCOPE

The scope of this study will concern itself with the two extreme forms of the four basic types of virtual communities identified in Chapter III: Open/legitimate communities and closed/illegitimate communities. The purpose in limiting the scope so is to permit a more detailed examination of the two most distinct “sides” of virtual life: the open side - characterized by communities of interest, civil society movements, virtual “states,” and

online gaming communities - and the clandestine side, characterized by so-called "darknets," criminals, terrorists, racists, and cults. Closed/legitimate communities (such as the military and intelligence communities) and open/illegitimate communities such as music file swapping p2p-based communities represent opportunities for further study.

E. METHODOLOGY:

To provide a basis for examining the issues, this paper first presents a review and discussion of the current literature on the subject of virtual communities and on-line behavior. From these sources, this study generates a working theory about the relationship between social behavior and social technologies and extracts a set of unique characteristics that describe intensive networkers and virtual communities. Using case studies, this paper then tests the validity of the theory and its predictions. The cases examined include the virtual world of *EverQuest*, America Online (AOL) chat rooms, online pedophiles trading in child pornography, and the Al Qa'ida terrorist network. In the cases of *EverQuest* and AOL chats, data is obtained through membership, observation and interaction. For obvious reasons, data relating to criminal or terrorist communities cannot be obtained through direct participation, and must instead come from other sources.

F. LEGAL ISSUES

In no way does this study conflict with existing intelligence oversight regulations and/or the privacy rights of the research subjects. Personal identities are masked in accordance with the wishes of research subjects, and to prevent abuse of U.S. citizens' personal information. Known, suspected or planned criminal activity revealed in the course of doing research (if any) has been reported to appropriate authorities. These measures may introduce a bias limiting the applicability and value of this study's findings; however, the author believes they are unavoidable and in any case, minimal.

G. ORGANIZATION

Chapter II provides a review and discussion of current literature on the technology and society, and presents a sociological theory of cyberspace. Chapter II also provides a list of definitions used throughout this paper. Chapter III is divided into two main sections; the first half of Chapter III examines the relevant literature regarding the virtual environments in which individuals operate: virtual communities. Chapter III classifies virtual communities in two dimensions: open vs. closed and legitimate vs. illegitimate and explores the distinctions. The second half of Chapter III develops a profile of the intensive networker, the "digerati," based on current literature and the characteristics of virtual communities examined in the first part.

Chapters IV, V, VI and VII comprise the case studies, and Chapter VIII presents conclusions and recommendations.

H. BENEFITS OF STUDY

The findings of this study will better enable the military to recruit and train "information operators," to more effectively structure military computer-mediated communications architectures, and provide insights into both our own networks and those of our enemies. These findings will better enable the United States to maintain superiority in the various aspects of information warfare and computer network operations fundamental to all combat and support activities.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE "VIRTUAL" SOCIETY

> *"This book studies the emergence of a new social structure, manifested in various forms, depending on the diversity of cultures and institutions throughout the planet. This new social structure is associated with the emergence of a new mode of development, informationalism, historically shaped by the restructuring of the capitalist mode of production towards the end of the twentieth century."*
>
> *- Manuel Castells. The Rise of the Network Society. p. 14*

A. INTRODUCTION

The current preoccupation with and development of information operations as a military doctrine and practice occurred in conjunction with the growth and spread of computer-mediated communications technologies (CMCTs). At first, the military treated information operations as specific to CMCTs. Then PSYOP, military deception, and Command and Control (C^2) warfare were included within the broad definition of information operations and information warfare:

> Information operations (IO) involve actions taken to affect adversary information and information systems while defending one's own information and information systems. They apply across all phases of an operation, the range of military operations, and at every level of war. IO capitalize on the growing sophistication, connectivity, and reliance on information technology. … IO target information or information systems in order to affect the information-based process, *whether human or automated*[1]

With regard to *information operations*, whether in the real world or in cyberspace, a distinction between what is virtual and what is real is meaningless. Technology is a mirror of society, but a necessarily imperfect one – exaggerating the importance of one aspect at the expense of another. Society redefines itself according to this self-perception. Post-modernist writer Sherry Turkel illustrates exactly the idea of societal self-redefinition in response to its technological reflection in Life on the Screen: Identity in the Age of the Internet (1995), discussing the perceived value of automated psychotherapy:

[1] Joint Publication 3-13, 9 Oct 1998. p. vii. Emphasis mine.

> In the case of computer psychotherapy, if computers can perform behavior modification, psychotherapy must follow. If computers can do cognitive mapping, this technique acquires new status. If the computer needs rules in order to work, then areas of knowledge in which rules had previously been unimportant must formulate them or perish (p. 107)

Turkel implies a certain amount of technological determinism; however, technological determinism is really a misunderstanding of the techno-social relationship.

The concept of "technological determinism" or the "technological imperative" is a teleological fiction. To imply that "technology" possesses agency is to anthropomorphize an impersonal phenomenon. Technology is the name humans give to a tool or the collective body of tools we use to accomplish human purposes. The teleology or agency implicit in the design or morphology of a particular tool has its origins with humanity. Because we design our tools – "technologies" – to help us accomplish specific purposes, they are necessarily limited in their functionality. It follows, therefore, that a given technology will facilitate some behaviors more than others, and perhaps even preclude altogether still other behaviors (i.e., it is difficult, if not impossible to weave cloth with a carpenter's hammer). To the extent that a society adopts and employs a given technology (which depends on that technology's utility), the use of that technology will reinforce some behaviors, and discourage others. Even technologies designed for purposes that are more general are still teleologically neutral. The same technology used to produce pesticides or vaccines is equally well suited to producing chemical or biological weapons. There is no technological imperative to produce either, both or neither.

One can find some support for the idea that technology has altered societies. One could find a parallel in how the rise of rail networks in the United States transformed the concept of physical property, much as information networks encouraged the further development of the concept of intellectual property (though did not invent it), and the sociological ramifications of these technology-inspired changes. Conversely, one can see how technologies *apparently* failed to alter some societies while radically changing others. For example, the wheel appeared independently in Western Europe and in the Andes Mountains of South America. In Europe, where the relatively flat to-

pography of the terrain enhanced the utility of the wheel, carts, carriages, bicycles, automobiles and ultimately car racing, traffic courts, and high-volume interstate commerce developed. The rugged topography of the Andes Mountains made the wheel of very little real utility to the Incas; therefore, the Incas transported loads by llama or on foot. The only utility wheels could offer in this environment was to entertain children as toys, hence no Peruvian autobahn. Since the wheel appeared in two widely separated societies, both in distance and in culture, yet molded the course of one while hardly affecting the other, it is hard to support the idea that somehow technology itself determines absolutely the shape of society. In *all* cases, the degree of the technology's assimilation, and its subsequent influence reflected *local* needs and conditions.

Many writers have argued that human society is in the process of completing a cognitive shift in our relative use of tangibles and intangibles. For example, one may trace this shift throughout the development of our economic system. It began with the shift from a barter economy to the use of currency. The shift continued with the invention of paper money in China in 650 A.D., the willful rejection of currency backed by gold in the early decades of the twentieth century, and within the last decade, the shift from tangible (if intrinsically worthless) currency to intangible electronically mediated transactions.

In their Foreword to John Arquilla's and David Ronfeldt's In Athena's Camp, entitled "The New Intangibles," noted futurists Alvin and Heidi Toffler (who first described the shift in our monetary systems in their book The Third Wave) point out that

> The same shift towards intangibility is evident in military affairs. In the past, intangibility in military matters usually referred to morale, leadership quality, courage, and strategic insight. Today, all of these remain important, but intangible assets include what is inside our databanks as well as the skulls of our soldiers. They include the power of software, the ability to blindside an opponent's information technology, the superiority of information collection and dissemination, the compatibility of information enhancing tools, and much more.[2]

Literature describing the emerging virtual society over the last ten years tends to grapple with the real-virtual/tangible-intangible distinction. The author posits that such

[2] Arquilla and Ronfeldt. (1997). p. xiv

distinctions are essentially meaningless. A paper document has no inherent value beyond the materials and labor that went into its construction; its true value lies in its information content, which is intangible anyway. Weighing the value of soft-copy against hard copy is ultimately weighing the value of one interface method over another. This value is, of course, determined locally.

Sociology, as an intellectual domain, has also followed the general trend. As sociologist Piotr Sztompka writes, there has been a recent paradigmatic shift in thinking about societies and cultures – from a "sociology of systems" to a "sociology of action."

> At the epistemological level, there is a corresponding turn from structural explanations invoking 'hard' variables – like class position, status, economic situation, demographic trends, settlement patterns, technological developments, organizational forms – toward cultural explanations focusing on 'soft' intangibles like meanings, symbols, rules, values, norms, codes, frames, and forms of discourse.[3]

B. A SOCIOLOGICAL THEORY OF CYBERSPACE

It is the author's contention that the creation of CMCTs is arguably in opposition to this trend. CMCTs give physicality to our social networks – the intangible made tangible, and therefore obvious. This fleshing out of the global amalgam of social networks is, at present, incomplete; however "thumb-tribes," intranets, LANs, Usenet groups, blogging communities, "virtual states" and web rings, to name a few, are *human* communities whose intangible qualities are incarnate in CMCTs. In essence, the use of CMCTs represents a trade-off. We make the object of exchange intangible, but require tangible means to use it.

Within a network, what matters are the "true intangibles," or more specifically, the metadata and meta-properties that describe the network itself, including topology and rules of interaction. There is no difference between a real and a virtual social interaction space; the meta-properties and metadata are simply more apparent and measurable – more "transparent" – in CMCTs.

[3] Sztompka. (1999). pp.1-2

All human organizations represent networks of differing topologies. As Hamman points out,

> Privatised communities take the shape of networks and network communities are more likely to be based upon individuals rather than in neighbourhoods. This shift towards private network communities, from communities rooted in a specific, confined geographic area, is due to the privatisation of public spaces once important to the development of community. In the absence of public gathering places of the type which often facilitate the development of geographically based communities, the internet becomes a practical, efficient, and valuable tool for interpersonal communication which is important to the continuance of private network communities which are based upon individuals.[4]

CMCTs merely reveal what was there all along and enhance its efficiency. Network science suggests that network formation is ubiquitous; the most efficient form of self-organization. The recent emphasis on network-centric operations is the result of the newfound transparency of our social and economic orders. They are transparent because CMCTs create a tangible infrastructure for them. New network mapping/influence modeling and visualization software can provide effective targeting tools for information operations by providing a cognitive framework for assembling and understanding the multilayered *metadata* which constitute the rules underlying network behavior, and which become the instrumentalities and objects of manipulation in information operations. *Therefore, cyberspace is ultimately no different from any other social space.* The supposedly novel features and problems of computer-mediated social organizations are analogous to those of already existing social organizations; their points of difference are attributable to interface methodology. Because interface methodologies (to include input/output devices, language, and software environments) vary with locality, they are understood poorly as a class.

Computer-mediated communications technologies are collectively an artificial reconstruction and embodiment of the social networks (the primal medium of information exchange) within which all human beings are embedded from birth. In contemplating its reflected image (CMCTs), society has become, gradually, collectively aware of its own pre-existing network structures, and of the ubiquity of networks – hence the explosion of

[4] Hamman, R. (1999).

recent popular research into networks: social, biological, computer-mediated and otherwise. The concepts of "network-centric warfare" and "swarming tactics" have emerged in no small part from this general recognition of the ubiquity of networks, and the advantages that derive from "pure" or "flat" network forms of organization.

All this suggests a theory of cyberspace that does not require a radical revision of human society. CMCTs provide an inherently neutral but polymorphic forum for human social interaction (cyberspace) – a virtual social environment analogous to the real environment. Behavior in this virtual realm mirrors behavior in the real world, that is, specific emergent social topology (real or virtual) depends on the local social needs of individuals and/or bounded groups (communities) – regardless of how those boundaries are drawn. Because of this, the spatial, temporal, and contextual boundaries of the real world tend to remain intact in the virtual world despite the existence of widely varying virtual habitués and the distance-transcending properties of CMCTs. Theoretically, the specific topology (real or virtual) therefore can be known (mapped), analyzed and targeted appropriately when conducting information operations, to include PSYOP, military deception, C2 warfare and especially unconventional warfare conducted by special operations forces in support of counter-terrorism, counter-insurgency, and nation-building operations.

For example: Social, cultural, and even temporal boundaries remain intact in the virtual world of *EverQuest*:

> Other common connections between players are physical or cultural *proximity* and previous shared gaming experiences. Most Scandinavian players do, for instance, know other Scandinavian players that they have met through the game. Here it is the shared language (Danish, Norwegian and Swedish are at least in their written form very similar), *time-zone* and *culture* in general that works as an *a priori condition for the development of the networks* – similar conditions that make Tony Soprano belong to a network of people hailing from Sicily. Sometimes the offline/online similarities mesh even more, as when a gaming society in a small Swedish town decided to take on EQ. It is not at all unusual to find groups of friends move from one game to another. In such situations, *the game simply becomes a new environment for a preexisting social network to inhabit.*[5]

[5] Jakobsson and Tyler. (2003). pp. 84-85. Emphasis mine.

Other studies have revealed how ethnic, gender and generational boundaries remain intact among blogging communities,[6] though instances of deception and assumed gender or ethnicity do occur. At the same time, the technology involved can set limits on social organization that can spawn communities that transcend traditional boundaries and/or create boundaries. However, even in their transcendency, the boundaries that delineate virtual communities are not evidence of the death of traditional sociology.

Regarding military organizations, the localized nature of the social interaction space can render centralized control of operations counterproductive. This is because all social organization, like politics, is local. Therefore, the various uses of CMCTs reflect *local* social realities and needs. CMCT does not "create" new societies, but rather facilitates social organization consistent with local perspectives.

An interesting concept concerning the military is *netwar*. As defined by John Arquilla and David Ronfeldt, netwar is "a comprehensive information-oriented approach to *social* conflict."[7] If our technological networks are the physical manifestation of our social connectedness, netwar is an important concept. Arquilla and Ronfeldt have led the charge among those demanding that our military must change its organization to match that of our enemies. According to them and other organizational theorists, hierarchical organizations, such as our military, must fail against networked organizations. This is because hierarchies are inherently concerned with their own organizational survival in the face of adversity. Networks transcend this need, because topology (organizational structure) can form, dissolve, and form again in different patterns, as appropriate to the problem confronting them. They are able to do this because they are based upon the metadata that describes the capabilities and connectedness of each member, rather than on fixed, doctrinally mandated topology of office and authority. *Survival is not dependent upon structure, but rather the reverse.* This presents an interesting problem for the military, because of the tension between maintaining order and discipline while remaining flexible. Recommendations abound about how to fix this, and this thesis makes

[6] Choi, H. (2003).

[7] Arquilla and Ronfeldt. (1997). p. 6. Emphasis mine.

several. However, without a thorough understanding of the military network and its metadata, and profound personal commitment on the part of every airman, soldier, marine, and sailor and every commander and civilian authority, the flexibility will always elude us. Hierarchies pass information up and orders down. Unfortunately, our technology can facilitate this process as easily as it facilitates distributed operations. Technology is not deterministic. This thesis seeks therefore to illuminate the ways in which networks, groups, and communities are able to exist without formal structure, and how the technological network facilitates this.

C. DEFINITIONS

Cyberspace: the social interaction space created by and within, and accessible through, computer-mediated communications technologies. In Preece's terms, the "virtual environment."

Identity Performance: The situationally negotiated and sustained portrayal of self. Per Hine, "the person might be thought of as a convenient shorthand for a more or less coherent set of identity performances with reference to a singular body and biography."[8]

Interface Methodology: The hardware and software through which one may access and experience a given sector of cyberspace.

Local: Of or possessing close spatial, temporal and/or contextual proximity to the subject.

1. *Spatially local:* Interactions occurring within a limited geographic area.

2. *Temporally local:* Interactions occurring within a given time interval.

3. *Contextually local:* Interactions occurring within a given context (cultural, ethnic, or topical).

Metadata: the information that describes and facilitates the functioning of a network; includes information about topology (links and nodes) and patterns of interaction

[8] Hine, C. (2000). p.49

and flows; information about the network that may or may not be contained explicitly within the network.

Network: Per Kadushin[9], the definition of a network is simple, consisting of "nodes," which generally are objects or people, and "links" the connectors (physical or associative) that define the ways in which the nodes relate to each other. The simplest network is a dyad, composed of two nodes connected by a single link. The link (or links) may connect Node 1 *to* Node 2 or Node 2 *to* Node 1 (directional), or may connect Node 1 *and* Node 2 (symmetric). For this reason, *flow* is a better term than link. Any two nodes may connect by multiple flows (multiplex relationships) of varying *strength*[10]. Beyond the basic dyadic relationship, there are additional layers or tiers, defined by their *degree* (or path-distance) from a given node. Nodes of Degree 1 connect directly with the index node; nodes of Degree 2 connect to the index node via the Degree 1 nodes. For the average individual, there may be from 500 to 5000 people of Degree 1 in their individual social network – primarily family and friends (named relationships), coworkers and acquaintances (generic relationships). Each of these relationships may be weak, strong, directional or symmetric, formal or informal, heterophilous or homophilous. Mark Granovetter described social ties as being either "strong" or "weak."[11]

In Granovetter's terms, strong ties are those that exist between family members and close friends. Weak ties connect acquaintances. Strong and weak ties may be of any degree (path-length), although strong ties are predominantly first-degree relationships, and weak ties are predominantly second or greater degree relationships. The terms bonding and bridging have also been used to describe strong and weak ties.[12] This study uses the terms bonding and bridging to describe these sorts of ties because they offer a more nuanced understanding with regard to networks.

---

[9] Kadushin. (May 2000).

[10] "… The strength of a tie is a combination of the amount of time, the emotional intensity, the intimacy, and the reciprocal services which characterize the tie" M. Granovetter. (1973). "The Strength of Weak Ties." American Journal of Sociology. 78:1360-80

[11] Granovetter, M. (1983).

[12] Kali. (2003).

Network Capital: Per Rheingold, "the ability to use the technological network to contact social networks and to make use of them to one's benefit," derived from one's access to network technology, technological literacy, and social networking ability (see Social Capital below).

Social Capital: According to Nan Lin[13], social capital comprises those resources accessible through social networks. These resources include wealth, power, connections, material goods (car, house, etc), symbolic goods (education, club memberships, reputation, etc.). Resources can be accessed through both direct and indirect ties. However, defining social capital this way makes it possible to define almost *anything* as social capital. Other researchers have defined social capital differently. According to Putnam, social capital refers to "features of social life – networks, norms, and trust – that enable participants to act together more effectively to pursue shared objectives…."[14] Per Kadushin, social capital is the ability of individuals to draw upon their position in a network.[15] Given these definitions, I define social capital as the measure of an agent's *embeddedness* within a social network, which serves as *the* primary resource. Social capital is the quantitative and qualitative measure of one's social connectedness. The resources accessed in this way are only indicative of a person's social capital; i.e., one cannot become wealthy, earn a reputation, buy a house, gain power, etc, but through accumulating and using social capital. Successful politicians, for example, must have an abundance of social capital. Hermits and recluses, on the other hand, lack social capital. One accumulates social capital exponentially in accordance with Reed's Law[16] as one invests time and attention to collecting and maintaining social contacts. One expends social capital when one draws upon the network and fails to reciprocate. Social capital may be lost should one fail to maintain relationships with others or engage in behavior that leads to a loss of trust.

---

[13] Lin, Nan. (2001). p. 43.

[14] Putnam. (December 1995). pp. 664-665.

[15] Kadushin. (May 2000).

[16] Reed's Law, named for researcher David Reed, states that the value of a network grows exponentially with the number of users, or $V = 2^n$, where n = the number of users. By extension, the value of one's social capital is determined in part by the number of social connections one has. [Rheingold, H. (2003). pp. 56-61]

Social Networking Ability: Social networking ability is the relative ability of the individual to internalize and act upon the metadata that describes the social network in which he or she is embedded in order to access other resources.

Trust: The willful action of surrendering control over a desired outcome to another person or object with the expectation that the desired outcome will be achieved, and the acceptance, tacit or express, of the attendant risk and uncertainty.

Virtual Community: A discreet (bounded) group of people who regularly interact socially through computer mediated communications technology, using a common interface methodology or in a shared virtual environment, to further common purposes or interests.

THIS PAGE INTENTIONALLY LEFT BLANK

III. LIFE IN THE VIRTUAL COMMUNITY

A. VIRTUAL COMMUNITY DEFINED

In the current literature, there is an ongoing debate about whether online groups constitute "true" communities. Much of this debate revolves around the definition of community, and how closely online groups fit the definition. Community, as defined in Webster's New World Dictionary of the American Language is

> 1. *a*) Any group living in the same area or having interests, work, etc. in common *b*) such an area 2. the general public 3. a sharing in common.

Clearly, the emphasis on what is local, as defined earlier, plays a large part in defining a community. Jennifer Preece points out, "sociologists make clear distinctions between groups, networks and communities."[17] For our purposes, *groups* have clear boundaries, but do not necessarily possess a collective sense of purpose or an effective division of labor. *Networks* may cross boundaries, but ultimately preserve them nonetheless. Each bounded part of the network may preserve a slightly different sense of purpose and therefore fail to coordinate effectively.

Communities, however, subsume groups and networks within a collective, shared purpose and identity. Communities can define roles and tasks, and coordinate effectively. Communities often develop a shared culture that supports a strong collective sense of identity and mutual trust. It is here that the debate lies. As virtual ethnographer, Christine Hine puts it:

> Their concern is with the level of commitment and responsibility which participants associate with online social formations. It is suggested that online formations cannot be considered communities when participants can simply log out or turn off when they choose. The level of connection and intimacy is insufficient to make participants members of a community, although they may feel as if they are. This type of social formation is a pseudo-community. Advocates and critics of the idea of online communities tend to end up arguing about the authenticity of online social formations in relation to their real counterparts in a way which often harks back to a romanticized view of traditional communities. There is, however, a wider dimension to this debate. Watson (1997) points out that although to

[17] Preece. (2000). p.18.

> speak of newsgroups as communities often 'feels right' to ethnographers and to participants, the term itself carries a considerable amount of cultural baggage. To say that something is or is not a community is to perform political work. *Arguing over whether online social formations map directly to those that occur either ideally or actually in offline settings may be a distraction from the study of whatever develops online in its own terms.*[18]

Robin Hamman, editor of *Cybersociology Magazine*, defines an online community as "(1) a group of people (2) who share social interaction (3) and some common ties between themselves and the other members of the group (4) and who share an area for at least some of the time."[19] Hamman's definition is simple, and can encompass a wide variety of online groups

Social technology researchers Preece, Maloney-Krichmar, and Abras define online community as "a group of people who interact in a virtual environment. They have a purpose, are supported by technology, and are guided by norms and policies."[20] Although Preece, et al, generally consider all groups online to be online communities, they offer a set of variables that more or less affect the degree of closeness felt by their members:

- Physical as well as virtual presence
- Purpose
- Supporting software environment (interface methodology/ forum)
- Number of members
- Life-span
- Stage in life-cycle
- Culture of members
- Governance structure and associated norms and rules

For the purposes of this study, virtual or online communities are ***discreet groups of people who regularly interact socially through computer mediated communica-***

[18] Hine. (2000). p.19. Emphasis mine.

[19] Hamman. (1999).

[20] Preece, et al. (2003).

tions technology, using a common interface methodology or in a shared virtual environment, to further common purposes or interests.

1. Forum vs. Community

A word about forums: As Preece, et al. note, the supporting software environment is crucial factor in communities online. Virtual forums represent a wide variety of *interface methodologies*, and may represent a basic point of distinction between communities. Different forums require different technical skills. For example: Those who participate in web-rings (inter-linked web sites, generally pertaining to a common interest) and bloggers (authors of web-logs, web-page based diaries) must exhibit skill with HTM and HTML formatting, coding and graphic design. Bloggers and members of web-rings may share graphics, sound files, references, and other resources with each other. Conversely, there is a certain amount of competition among web-site producers. In such competition, one measures success in terms of numbers of visitors to one's site, and various web-publishers compete with others in their community for the attention of other members as well as the attention of casual surfers and of companies potentially seeking their talents and skills. In contrast, individuals who participate in Multi-User Dungeons (MUDs) like LambdaMOO are generally familiar with programming language and prefer to operate in a DOS-like, text-based operating environment supported by TelNET. Many construct their own virtual "rooms" filled with virtual objects that have various virtual characteristics, all created and described through the rules of the MOO's programming language. Of concern for the MUDs and MOOs is the fact that programmers can enact virtual crimes such as the often-cited instances of virtual rape.

A non-comprehensive list of such forums includes:

- Web rings/Blogging circles
- Chat groups (IRC, AOL, The Palace, and others)
- User-owned and regulated text-based MUDs and MOOs
- Commercially owned and regulated graphics-based Massively Multi-Player Gaming Communities (*EverQuest*, The Matrix Online®, etc.)
- UseNET, Newsgroups and BBS
- E-mail networks
- Web-based discussion groups (Yahoo! groups)

- IM-based groups (AIM, Huminity, Buddyspace, Jabber)
- Distributed computing projects (Climateprediction.net, SETI@home)
- Peer-to-peer (p2p) file-sharing networks (Kazaa, Napster, Gnutella)

The above list serves as the list of potential virtual communities to explore in case studies. This is not to say that interface methodology is the key discriminator among virtual communities. Such forums constitute the different forms cyberspace can take; however, the technical existence of such forums does not imply community. Community is a *social* phenomenon, and emerges exclusively from the patterns of *human* interaction that occur in these forums, which are determined by the local choices of members, of which interface methodology is only one.

2. Communities of Interest and Communities of Practice

Another distinction exists that must be explored briefly. One can find any number of websites advertising interface methodologies and software to support *communities of practice*, that is, identified preexisting communities that may enjoy the benefits of a tailored CMC infrastructure. Communities of practice are businesses, government agencies, churches, and other institutions whose primary purpose is to carry out some function. The military is one such community. The vast majority of online communities that occur in cyberspace are not communities of practice, but rather *communities of interest*. Even online political or social action communities are not communities of practice, because members generally do not earn their livelihoods through membership in those communities. Communities of practice may be better understood as closed/legitimate communities, per the typology in the following section.

Members of such communities are likely to be among the first *true* net-*workers*. These are the mobile professionals. It is for these people that local area networks (LANs) wide area wireless networks (WANs), laptop computers, cell phones and PDAs were originally conceived. In a very real way, communities of practice collectively serve as the early adopters or innovators of networking technologies, and whose conspicuous use of such technologies serves to spread successful technologies into the larger com-

munity of late adopters. Commercial or corporate communities of practice deserve to be studied in their own right, and may provide the best model for the routine use of CMCT in the military. However, because the military itself falls within this class of communities, this study excludes such communities in the interest of exploring dissimilar perspectives.

B. A TYPOLOGY OF VIRTUAL COMMUNITIES

Online communities come in many varieties, although as we have seen, each traditionally is classified according to interface methodology. However, when one is able to strip away the *technique* (graphical or text based interfaces; programming or plain language interfaces; PC or mobile device) to look at the social underpinnings, a different pattern emerges. Two dimensions appear: One continuum runs between open or closed, which is determined by the rules or conditions governing accessibility and membership. The other continuum lies between legitimate and illegitimate, depending on the type of behavior its members engage in, or the purpose for which they exist as a group (Figure 1.)

The Federal Bureau of Investigations' Cybercrime Division recognizes one of these dimensions. According to their Operation Candyman website,

> These groups can be 'closed' or 'open' communities. In a closed community, a member of the group must invite you in and non-members searching the Internet cannot identify the identity of the group. In open communities, such as 'Candyman,' any person searching the Internet can conduct a search by title or category, locate the group, and may be granted membership by the monitor of the group. The monitor may be the creator of the group or a member selected by the group.[21]

[21] "Innocent Images Operation Candyman Phase I." (March 18, 2001).

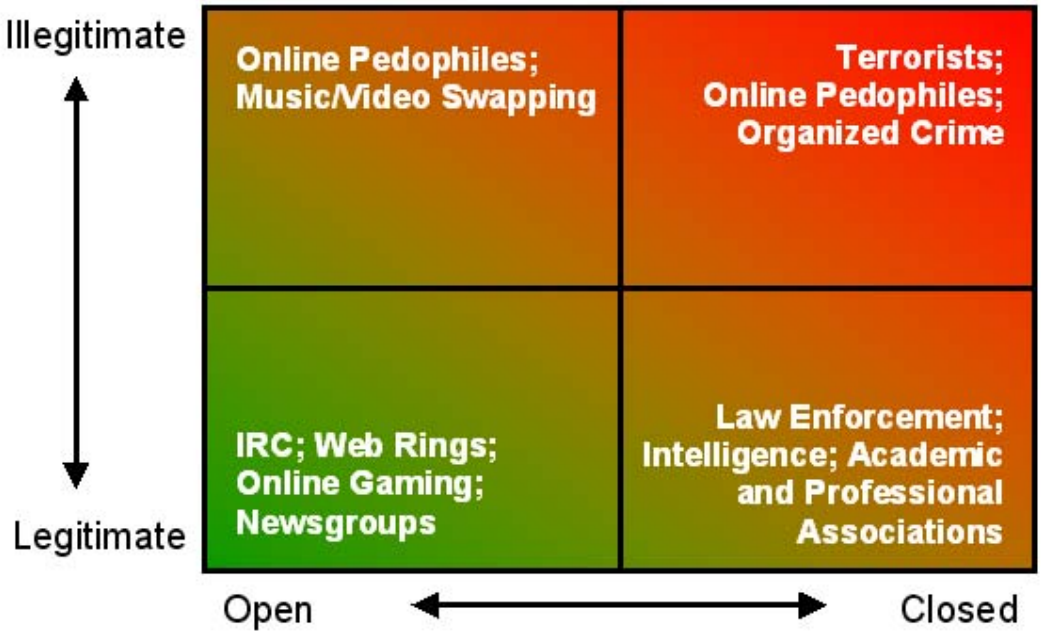


Figure 1. Typology Matrix of Virtual Communities.

The FBI's characterization is qualitative, rather than quantitative, in keeping with Sztompka's "sociology of action." However, the FBI's definition is one-sided and lacks nuance as well as predictive capability. A child porn group is illegitimate but can be open or closed as the FBI notes. A group of law enforcement officials or intelligence officers may be closed but would be legitimate. Similarly, a nodal analysis of such networks may be useful for identifying members for arrest or targeting, however, it fails to address the larger issues involved, the metadata of the network and the mode of connectivity and thus fails to generate a suitable model for thoroughly understanding such communities.

The scope of this study will concern itself with the two extreme forms of the four basic types of virtual communities identified in Chapter III: Open/legitimate communities (hereafter called open communities) and closed/illegitimate communities (hereafter

called clandestine communities). I use the term clandestine because it more accurately reflects the character of closed/illegitimate communities. The term "closed" is not sufficiently descriptive. "Clandestine" or even "covert" are better choices, although the term "covert" implies a certain degree of deception about the group's identity, nature, and purpose that frequently is not there – although some groups do engage in covert activities. Clandestine preserves the secretive nature of such groups.

The purpose in limiting the scope so is to permit a more detailed examination of the two most distinct "sides" of virtual life: the open side - characterized by communities of interest, civil society movements, virtual "states," and online gaming communities - and the clandestine side, characterized by so-called "darknets," criminals, terrorists, racists, and cults. Closed/legitimate communities (such as the military and intelligence communities) and open/illegitimate communities such as music file swapping p2p-based communities represent opportunities for further study.

An issue that arises frequently in various other descriptions of online communities is the issue of governance, norms and policies (Rheingold, 2003; Preece, 2002; Lubeck, 2003; Hine, 2000). I will address these issues only insofar as they appear in the specific communities covered in the case studies. Governance is *always* specific to the community; although some norms and policies reflect the broader cultural and legal context, in which the membership is embedded. Prohibitions against profanity, lewd or lascivious conduct in public forums are examples of these types of policies. Striving for social equality or balance is another value that may be enforced. In addition, the interface methodology will influence the *negotiated* norms that arise within communities, such as the use of emoticons (ASCI character combinations that resemble facial expressions), the avoidance of all upper-case text inputs, or social disapproval and social sanctions against those who engage in deviant behavior. For these reasons, governance is predictive only in specific cases, and do not represent a general feature of online communities beyond the fact of their existence.

1. Open/Legitimate ("Open") Communities

a. Characteristics

For the purposes of this study, an open/legitimate community is one that is possesses the following five characteristics:

1. Purpose: Sociability, political or religious discussion and fellowship, legitimate sociopolitical activity and debate, entertainment, legitimate information exchange, and commerce. *Organizing Principle* is an important related concept, although it is not necessarily synonymous with Purpose.

2. Broad Accessibility: No special access negotiations are required; anyone can join.

3. Trust: Members are content to accept the identity performances of members at face value. While identity play is present, it exists in accord with community norms. In open/legitimate communities, widespread trust among all members is not an issue or is less an issue – there is little risk in network participation and hence little need for trust. When the risk gets higher, then people turn to closed communities of people they trust. Because anyone can join an open/legitimate community, there is little or no concern about credentials and other indicators of trust in terms of membership – but credentials may matter over time in terms of influence within the community.

4. Mode of Connectedness: While strong (bonding) ties may develop, weak (bridging) ties usually predominate. There is a rough correlation between the size of the group and the strength of ties. Small, homophilous groups tend to experience stronger ties than large heterogeneous ones. The emphasis is on connectivity as opposed to exclusivity.

5. Persistence: Dependent variable. Successful open communities have an aggregate interest in maintaining the community for extended periods, although the life spans of virtual communities vary widely – anywhere from a few weeks or months to many years.

b Examples

Examples of open communities abound; they are the types of communities to which the vast majority of Internet users belong (see list, p.31). In communities such as *EverQuest*, identity play for entertainment purposes is actually the *raison d'etre* of the community. Although *EverQuest* allows users to mask their identities, most players do not, preferring instead to be able to "step out of character" whenever convenient

in order to chat with other players. It is a given that the characters one encounters while traveling about the *EverQuest* realms are unlikely to be true representations of the players.

In some chat communities, there can be significant pressure to portray oneself realistically. Real friendships can develop among participants and it is often personally devastating when trust is violated in this manner. The apocryphal example appears in Stone's 1991 essay, "Will the Real Body Please Stand Up:"

> After several years, something happened that shook the conference to the core. 'Julie' did not exist. 'She' was, it turned out, a middle-aged male psychiatrist. …He had spent weeks developing the right persona. A totally disabled, single older woman was perfect. …It worked for years, until one of Julie's devoted admirers, bent on finally meeting her in person, tracked her down. …Reactions varied from humorous resignation to blind rage. Most deeply affected were the women who had shared their innermost feelings with Julie. 'I felt raped,' one said. 'I felt that my deepest secrets had been violated.' Several went so far as to repudiate the genuine gains they had made in their personal and emotional lives. They felt those gains were predicated on deceit and trickery. [22]

Perhaps what characterizes open communities the most is the expectation of openness on the part of the other participants, and the willingness to engage in trusting behavior.

2. Closed/Legitimate Communities

a. Characteristics

A closed/legitimate community is one that is possesses the following:

1. Purpose: Legitimate information exchange, discussion, and commerce. Also professional, academic, or industry-related interaction, collaboration, research and operations.

2. Restrictive Accessibility: Only vetted (more or less thoroughly) individuals are admitted to participate and efforts of varying degree may be made to conceal servers, data flow patterns, and information exchanged.

3. Trust: Security and/or integrity (quality of content and/or interaction) are the primary issues for these communities. Encryption may be employed. Ano-

[22] Stone. (1991). p.1.

nymity is discouraged in favor of authenticated identities. Generally, all closed communities distrust outsiders to some degree. New members and/or their contributions must be vetted before they are permitted access or otherwise accepted.

4. Mode of Connectedness: Bonding ties usually predominate, although there is a healthy complement of bridging ties as well. Exclusivity is valued.

5. Persistence: Dependent variable. Successful closed/legitimate communities have an aggregate interest in maintaining the community for extended periods, although the life spans of virtual communities vary widely – anywhere from a few weeks or months to many years.

b. Examples

Closed/legitimate communities are usually what we have called earlier communities of practice. The law-enforcement community, the military community, and the intelligence community are some examples. Professional and academic associations fall into this category as well. This study will not cover closed/legitimate communities in any depth, because its purpose is to look outside the type of community to which the author belongs at the three other types to see if there are any features or practices that may be of use within the military and intelligence communities.

3. Open/Illegitimate Communities

a. Characteristics

An open/illegitimate community is one that is possesses the following:

1. Purpose: To engage in unsanctioned or prohibited activity for which participants may be punished. Such activities range from dissidence, software piracy, and copyright infringement to consumer fraud and child pornography.

2. Concealed Accessibility: Minimum efforts are made to conceal identities and hide activities; security is generally poor. Any person with the proper knowledge, skills, and/or equipment can gain access.

3. Trust: Trust among members is generally a non-issue, although prospective members may encounter a nominal vetting process. Trust in the ability of the system to conceal identities and activities is a greater issue, although only minimum efforts are made.

4. Mode of Connectedness: While strong (bonding) ties may develop, weak (bridging) ties usually predominate. The emphasis is on connectivity and less on exclusivity.

5. Transience: Dependent variable. Open/illegitimate communities have an aggregate interest in maintaining security. They often employ technologies or techniques (such as p2p) that permit rapid, ad-hoc organization and disbanding.

b. Examples

Certain communities of online pedophiles and various networks that exchange copyrighted or proprietary information and data (music files, video files, and assorted "warez") are open/illegitimate communities. This study does not address open/illegitimate communities, per se, except insofar as communities of online pedophiles occupy the gray region of the continuum between closed and open.

4. Closed/Illegitimate ("Clandestine") Communities

For the purposes of this study, a closed/illegitimate or clandestine community may be distinguished by the following set of characteristics:

a. Characteristics

1. Purpose: To engage in unsanctioned or prohibited activity for which participants may be punished. Such activities include organized crime, terrorism, insurgency, and child pornography.

2. Restrictive Accessibility: Only vetted (more or less thoroughly) individuals are admitted to participate; conversely, strong efforts are made to ensure complete anonymity of participants, and to conceal servers, data flow patterns, and information exchanged.

3. Trust: Security is a primary issue. Encryption, steganography, and anonymity are widely employed. Generally, all closed/illegitimate communities distrust outsiders. Frequently, distrust remains a factor even within such communities, albeit to a greater or lesser extent depending on the community. The issue is whether there is a need for trust. Closed-illegitimate communities operate in a risky environment that demands trust. They operate in closed nets where members must be vetted before they are trusted.

4. Mode of Connectedness: Bridging ties are minimized and bonding ties predominate.

5. Transience: Dependent variable. Closed/illegitimate communities have an aggregate interest in maintaining security. They often employ technologies or techniques that permit rapid, ad-hoc organization and disbanding.

b. Examples

Clandestine networks, such as those formed and employed by Islamist terrorists, are strongly homophilous. Strong (bonding) ties are probably more likely to be found in homophilous communities than in heterogeneous communities. In clandestine communities, "trust" is predicated upon guilt and threat. If one wants to join a certain community of pedophiles, one must agree to upload illegal material. If one wants to join a terrorist group, one must commit illegal acts of violence. If one wants to rise within the mafia, or a street gang, one must commit a felony. The commission of these crimes *binds* one to the organization, both as a demonstration of one's personal commitment and as a point of leverage the organization can use against the prospective member. At any point, one can choose to defect, but the potential negative consequences (i.e., arrest and conviction, loss of life, loss of family's life, loss of wealth) tend to discourage defection. This is not cooperation and coordination based on *trust*, but rather upon *coercion*. However, there is also trust because of the risk, especially trust from those lower down in the ranks of those higher up – the foot soldiers have no coercive power over the leaders – the leaders have to trust them or get rid of them. In clandestine communities, one is assumed to be untrustworthy unless and until one can be bought, blackmailed or prosecuted (in which case trust is placed not in the person so much as in the strength of their baser instincts and urges – greed, self-preservation, etc.); or unless one has family members in these groups, long-time relationships with existing members, or other preexisting strong ties. In the case of Islamist terror groups, shame and guilt are employed to great effect, often without any self-conscious sense of their own hypocrisy

Clandestine networks exist primarily to carry out strongly prohibited (or at least unsavory) activities, thereby ensuring the premium placed on security (although

many pedophiles have been arrested because they thankfully failed to pay enough attention to security). Valdis E. Krebs, designer of software used to graphically map social networks applied his expertise and software (InFlow©) in an innovative study of the 9/11 hijackers' networks. Significantly, Krebs found that

> Covert networks often don't behave like normal social networks (Baker and Faulkner, 1993). Conspirators don't form many new ties outside of the network and often minimize the activation of existing ties inside the network. Strong ties, which were frequently formed years ago in school and training camps, keep the cells interconnected. Yet, unlike normal social networks, these strong ties remain mostly dormant and therefore hidden. They are only activated when absolutely necessary. Weak ties were almost non-existent between members of the hijacker network and outside contacts. It was often reported that the hijackers kept to themselves. They would rarely interact with outsiders, and *then often one of them would speak for the whole group*. A minimum of weak ties reduces the visibility into the network, and chance of leaks out of the network.[23]

Other communities of violators such as certain groups of online pedophiles and music swappers (open/illegitimate communities) rely less on strong pre-existing social bonds and more on anonymity and direct, rather than mediated, access to files on other participants' computers. This is another version of the strong tie: first degree, rather than second-degree connectivity.

C. WHO NETWORKS? PROFILE OF THE ON-LINER

Most of us would not consider ourselves members of the "digerati," no matter how regular and frequent our forays into cyberspace may be. For example, a certain friend of mine has been venturing into cyberspace since the mid 1980's, participating heavily in some of the original Bulletin Board Systems (BBSs), building and modifying his own computer systems, and maintaining an extensive online network of personal acquaintances. Today, he works for a defense contractor installing networks and dabbling in network security. However, he does not consider himself a member of the digerati. Who then are the digerati, and what makes them so special?

[23] Krebs. (2002). Emphasis mine.

A recent study by the University of California, Los Angeles has, in the words of Reuters wire service, "shattered" the "stereotype of the loner 'geek' who spends hours of his free time on the Internet and rarely engages with the real world."[24] According to the UCLA Study press release,

> In every country in the World Internet Project, Internet users watch less television than non-users…. In contrast to television viewing, Internet users in all of the surveyed countries spend *more time* than non-users in social activities. Internet users in all of the surveyed countries spend more time or as much time as non-users socializing with friends or exercising, and spend more time reading books in all of the countries except Germany and the United States.[25]

Beyond dispelling the "geek myth," the study reveals other interesting facts, attitudes and beliefs about users' interaction online:

- Most users *disagree* that by using the Internet, they can have more say about what the government does.
- Most users *disagree* that by using the Internet, they can better understand politics
- Most users say that the use of Internet did *not* affect, or only very slightly increased, their contacts with family, friends, or people who share their political interests, religion, or profession
- With the exception of Morocco, Chile, and China, most countries' Internet users had at least five years of experience in its use.
- The average number of online friends met in person ranged from 0.6 in Japan, to 2.3 in Spain. Conversely, the average number of online friends *never* met in person ranged from 1.1 in Japan to 7.7 in China. Older users tended to have far fewer online friends than younger users. Men were more likely than women are to use the Internet, have online friends, and to seek in-person contact with them.
- Wealth and possession of a college education *strongly* affected Internet use.
- Accessing the Internet from home dominated all other locations, including at work and at school.

[24] "New Study Shatters Internet 'Geek' Image." (14 January 2004).

[25] Lebo and Wolpert. (14 Jan 2004).

- 41 percent of users in the United States spent 10 or more hours online each week, although only 28 percent of users did so from home. In all countries, hours spent online only weakly correlated with age, younger users spending more time.

The UCLA data suggests that most Internet users are young males (ages 16-24), who come from relatively affluent (fourth quartile), educated families, or who are relatively well off and college-educated themselves. Most users had at least a few years' experience using the Internet. Most users see the web neither as a vehicle for political action nor as a primary venue for socializing.

1. Network Capital

In his 2002 book Smart Mobs: The Next Social Revolution, Howard Rheingold introduces the concept of *network capital*, "the ability to use the technological network to contact social networks and to make use of them to one's benefit" (p.195). The concept of network capital as an individual characteristic is an interesting one, with implications beyond Rheingold's definition. For the author, network capital requires three components: *access to network technology, technological (computer) literacy*, and, perhaps most importantly, *social networking ability*.

a. Access to Technology

Access to technology simply means that the individual in question has the opportunity to use computer-mediated communications technology. Such opportunity presupposes a few things about the individual: He or she is either wealthy enough to purchase a network-capable device and access to a service provider, or is wealthy enough to at least purchase access to a connected device (in cyber cafes, for example); or he or she works for an employer or goes to a school that is wealthy enough to provide access. The individual must have some knowledge of the potential gain that access affords (otherwise he or she would likely not attempt to gain access); hence, he or she probably has some education.

b. Computer Literacy

Access to CMCT is only part of the story. To enter cyberspace and thereby engage in social behavior, our cybernaut must have at least a working knowledge of the technology. He or she must be computer literate. The literature available offers little in the way of definitions, and even less information on appropriate measures of computer literacy. Representative of the most common definition is the one expressed by Dr. Nancy Csapo, of Central Michigan University:

> Computer literacy usually refers to the ability to use a few commercial applications and touch-type smoothly (Rothstein 1997). Computer literacy can be defined as 'having a basic understanding of what a computer is and how it can be used as a resource' (Nichols 1998). Requirements for computer literacy vary, but may include an understanding of the basics of hardware, computer systems and ethics as necessary skills.[26]

However, in the information age, the truly computer literate must necessarily possess far more than a simple knowledge of what a computer is and an appreciation of its potential. Angela Smith, at the University of Michigan, offers a more sophisticated definition of computer literacy with three elements:

> First, digital technology requires users to understand how to negotiate strategically through non linear and non sequential text. The complexity of negotiating through text (and creating text) in multimedia/web-based environments often requires us to be strategic locators of the most appropriate text for our needs.
>
> (Second) The large amount of information and relative ease at which we can retrieve it also amplifies the need to (be) critical about (its) relevance, worth, and reliability.
>
> (Third) The tremendous flexibility, variety, and power digital technology gives us in finding and creating text also puts further demand on (users) to analyze and create text for a variety of purposes and audiences.
>
> The three elements of critical technological literacy discussed—multimedia/ hypertext comprehension (and navigation) strategies, information-finding strategies and critical use, and the increased necessity of allowing

[26] Csapo. (August 2002).

> students to explore and create a wide variety of texts—give us a rough idea about the challenges vanguards of literacy face in the 21st century.[27]

Smith's definition is somewhat convoluted, but put simply: Computer literacy requires specific cognitive skills (critical analysis[28] and mental flexibility) and technical abilities (computer operation and Web navigation). Most Internet users have at least this level of competence. Web page producers, bloggers, MOO and MUD members all possess better than this base level of computer literacy. However, to be able to use CMCT to its full capacity – to organize socially and politically, one final element remains.

c. Social Networking Ability

All of us are embedded within social networks from birth until we die. It is within our various social networks that we become acculturated, socialized, educated, find or create opportunities for advancement, organize, and in which we are driven to find our place. Social networking ability is the skill that permits the individual acting alone to enjoy the benefits of membership in a community. Kali describes:

> A number of recent papers have adopted the view that social capital is embedded in social networks. An increasingly persuasive body of recent research argues that humans are embedded in social structures and that they choose actions taking account of the social contexts in which they live. [29]

Taken with Kadushin's definition of social capital (see Chapter 2), social networking ability is the relative ability of the individual to internalize and act upon the

---

[27] Smith. (Spring 2000).

[28] Interestingly, according to the UCLA World Internet Project, "in most of the countries in the UCLA World Internet Project, more than half of Internet users say that 'most or all' of the information they find online is reliable and accurate. Users in Korea have the highest level of trust in online information, with 69.7 percent saying that most or all of the information on the Internet is reliable and accurate. The least-trusting Internet users are Swedes; 36 percent said that none or only some of the information online is reliable and accurate, followed by Japan (25.3 percent), Germany (18.5 percent) and Singapore (18.3 percent). In the United States, 53.1 percent of users say that most or all of the information they find online is reliable and accurate, while 7.1 percent say that none or only some of the information is reliable and accurate."

[29] Kali. (January 2003). p.5.

metadata that describes the social network in which he or she is embedded. This then is the final element of network capital.

Researcher Karen Stephenson and author Malcolm Gladwell have names for people with a knack for this skill: hubs, gatekeepers, and pulsetakers,[30] or connectors, mavens, and salesmen. [31] Although Stephenson and Gladwell differ slightly in their explanations of these types of people, one can make rough pairings, as above. "Hubs" (Stephenson) and "Mavens" (Gladwell) are those who know where the best resources are and act as resources for information and ideas. Hubs have more connections (links to others) than others do. "Pulsetakers" (Stephenson) and "Connectors" (Gladwell) are those with a great number of weak (bridging) ties across divergent groups and interests. "Gatekeepers" (Stephenson) and "Salesmen" (Gladwell) are not equivalent, however. For Gladwell, Salesmen are the people with an unusual talent for empathic leadership, who can evoke enthusiasm and trust in others. Stephenson's "Gatekeepers" are a hybrid of Hubs and Connectors, who are aware of their own worth to the network. Unlike the other aspects, which tend to be more social qualities of the people who operate in networks, being a gatekeeper is related directly to one's position in the network, but not directly attributable to one's skills or social knowledge.

2. Trust

Trust is a vital component of virtual life: trust in the technology and trust in those with whom we interact online. Two important points about Trust emerge from the body of literature: authenticity as the basis of trust, with identity (or identity performance) and reputation as key factors in determining authenticity; and the need to cooperate and coordinate as the requirement for trust. Without the need to cooperate and coordinate, there is no need to communicate, no need to do so at a distance, and therefore no need for trust-at-a-distance.

[30] Kleiner. (October-December 2003).

[31] Gladwell. (2002). pp. 30-88.

This study concerns itself primarily with the authenticity aspects of trust. My observations indicate that, at least in its social role, online trust most closely resembles the formulation used by Murphy and Manjhi:

> The concept of what constitutes trust has been widely studied in areas like philosophy, economics, psychology and sociology. It has come to mean different things like personal trust, ('I trust that my parents would always do things for my own good'), trust because of good actions in the past, trust because of the perceived utility and trust because of one's perception about others. The notion of trust that we use in this work is to associate a principal with the good/bad actions it has committed in the past, and to use past behavior as an indicator of the future behavior. Clearly, the idea of *identity* is central to this notion of trust.[32]

In truly open communities, authenticity is irrelevant to membership – after all, anyone can join, and people join anonymously. There is no vetting. Authenticity may become relevant over time in terms of whether a member has influence in the community. In clandestine communities, however, even after authenticity has been established, full and complete trust is seldom granted – with the possible exception of trust between members who have a shared, positively perceived history together in real life and know each other quite well.

a. Identity Performance

Because text-based CMC – as such – lacks the subtle nuances of face-to-face communication, CMCT users are finding other means of confirming identity and verifying trust. For example, as ethnographer Christine Hine, researcher and author Jenny Preece and others point out, *netiquette* – the norms and rules of on-line social interaction – has arisen out of necessity. These norms vary depending on the specific group and virtual environment. For example, in many text-based environments, one generally does not type in all capital letters (the textual equivalent of shouting) nor should one change one's distinctive font (the text equivalent of changing one's voice). Consistency in the subtleties of on-line identity performance, peculiar to the interface method, is key to identity construction and to building and maintaining trust. The overall

[32] Murphy and Manjhi. (April 29, 2002). p.3.

pattern of behavior is the same in face-to-face and computer-mediated communication – we look for consistent, recognizable characteristics to confirm identity and verify trust.

In commercial interaction, however, these cues are not enough. The "authenticity problem" has provoked much innovation. Reputation systems like those on e-bay, Amazon.com, and Epinions draw comment from tech writers and do much to serve the trust-grounding needs of their customers. Certain software developers are creating and promoting identity-persistence software that equates to a net-wide roaming profile. These systems are nothing more than an automation of (until now) mostly informal reputation systems, or the salesclerk asking for photo-identification along with one's check. (Identity-theft is not a new phenomenon either.)

As Christine Hine puts it, "(One should) come to understand how it is the informants judge authenticity."[33] So, what constitutes "internet savvy" (grounds for trust)? Many, if not most people with any experience online pay close attention to consistencies such as text font & color, "speech patterns" (grammar, spelling, euphemisms, themes), use or disuse of emoticons, e-mail addresses & URLs, screennames/handles, and frequency of interactions to verify the identity of those with whom they communicate. Many use these same cues manipulate perceptions of their own identity (the use of the reflexive third person in online postings to lend credibility, or re-writing packet headers to spoof an IP address, for example). None of these indicators is foolproof, but in the absence of detailed technical knowledge of communications protocols, routing, and similar kinds of information about the systems they use, these contextual cues are the next most reliable indicators of trustworthiness. Many detectives hunting online pedophiles pay attention to these cues to construct believable personas with which to lure their prey. The use of all of these cues in the portrayal of authentic identity constitutes one's identity performance.

Assurances of benevolence (caring) and histories of competence can be incorporated in one's identity performance, which is the portrayal of self that one attempts to convey online. When the average user engages in interaction with another, he or she does not necessarily take the time to do a criminal background and credit re-

[33] Hine. (2001). p.49

cords check on them, or to request references from five of their closest friends to determine that they are who they say they are. If their identity performance is consistent over time in the course of their interaction, and the other can convince our user of their sincerity, competence, and benevolence (even if untrue), he or she will accept that identity performance as authentic. If the other's identity performance consistently indicates that the other is insincere, incompetent, and malevolent (even if untrue), the user will accept this portrayal as authentic and respond accordingly. More sophisticated users, however, may be technically informed and even proficient at tracing back IP addresses and/or "fingering" e-mail originators to verify authenticity.

The idea of "identity performance" comprises all three of Sztompka's factors: appearance, performance, and reputation.[34] You can look trustworthy, act trustworthy, and be reputed to be trustworthy online, without that characterization being actually true, and yet others will behave as though it is true until such time as they are given reason to change their assessment. Because it incorporates present and past behaviors, this particular model of trust also supports the "tit-for-tat" solution of the prisoner's dilemma. One grants trust when others merit trust. When others merit distrust, trust is revoked.

b. Cooperation, Coordination and Power

The need to trust others online is also necessary if participants in online communities have a shared sense of purpose. No single participant is capable of achieving the group's objective. In this sense, trust is necessary for overcoming the free-rider problem and solving the "prisoners' dilemma." Reputation systems, formal or informal, serve to curb free riders and multiple methods of communications, both online and off, facilitate cooperation and coordination. The purposes that can be achieved through coordinated action and cooperation may be laudable or deplorable, and many sources on this subject can site instances in which trust is essential to cooperation and coordination, as well as to personal success in any social group.

[34] Sztompka. (1999). pp. 71-81

> On the one hand, generalized distrust prevents people from engaging in social interactions. …Their unwillingness to engage in social interactions prevents them from improving their social intelligence. Their lack of social intelligence or social shrewdness, in turn, makes them vulnerable in such risky but potentially fruitful interactions.[35]

Rather than being deterministic of social practice, the need for reputation systems and identity-persistence software are instances of technological innovation driven by, and reflecting, enduring social factors. In addition to providing for successful coordination and cooperation, such systems provide for still other basic human social needs and drives, such as power. Those who seek to impress limits on identity performance on the Web are simultaneously constructing identity repositories (databases) under the control of commercial interests – not the control of the individual user.

3. Psychosocial Factors

a. Education and Wealth

According to many researchers studying the demographics of the Internet, wealth and education are the most prominent factors in assessing who has access to CMCTs, and who is likely to use them and/or be capable of using them. This particular point is generally undisputed, and can be illustrated with one or two quotes:

> Worldwide, 30 percent of Internet users had a university degree, and the proportion increased to 55 percent in Russia, 67 percent in Mexico, and 90 percent in China. In Latin America, 90 percent of Internet users came from the upper income groups. …In the United States, households with incomes of $75,000 and higher were 20 times more likely to have Internet access than those at the lowest level of income. *People with a four-year* college degree had a usage rate of 61.6 percent.[36]

> Disparities in computer literacy … can be traced directly to differences in educational attainment. For high-income countries, close to 60% of the college-age population was enrolled in college in 1998. By contrast, only 6% of eligible students in low-income economies enrolled in some type of

[35] Yamagishi. (2001) pp. 121-122

36 Castells, M. (2000). pp. 377 and 382. Emphasis mine

college or university program in 1998. These days, deficiencies in educational attainment are tantamount to deficiencies in computer literacy, a key determinant of the digital divide. [37]

b. Cognitive Ability and Information Needs

The Internet and the World Wide Web comprise terabytes of data. Not all of this data is reliable or even believable. Different people have different capacities to process information. In some cases, high-functioning individuals may be able to make good decisions on relatively scant amounts of data; others may require high amounts of data before they can make decisions. There is a point at which any mind can be overloaded with data, and at which performance declines. (See Figure 1.) Those among the digerati are fully comfortable sorting through the myriad formats and forums, and at judging the reliability of the information they find. It is precisely this high cognitive ability that makes possible their high technological literacy, and allows them to internalize vast amounts of metadata.

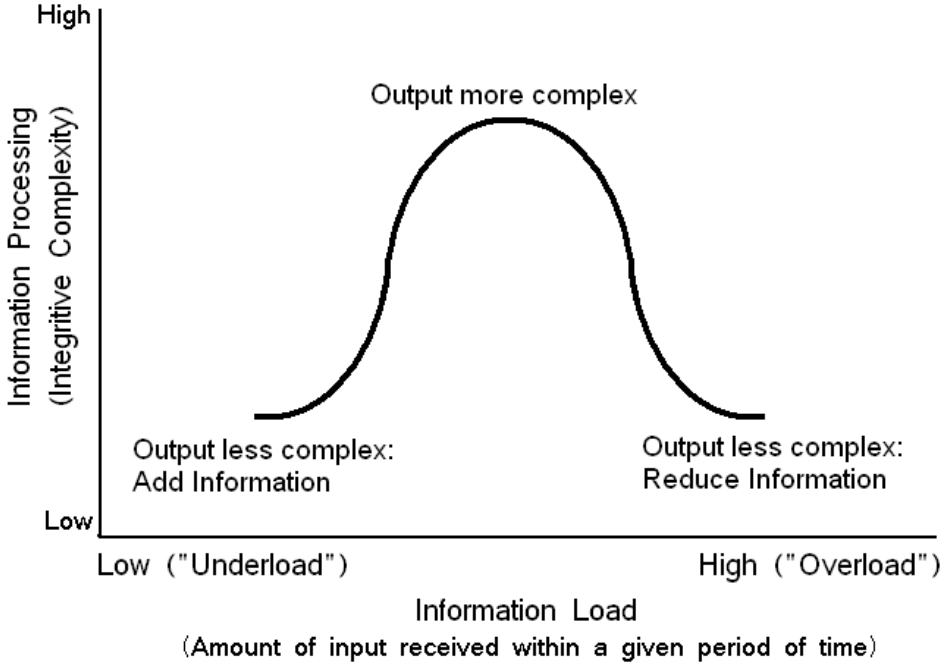


Figure 2. Relationship between the Complexity of Information Presented to a Decision-Maker and Capacity to Process Information (Source: Jansen. 2003.)

[37] Roach. (June 28, 2000).

D. CONCLUSION

Online communities and the people that participate most successfully have certain characteristics. To review:

Cyberspace is a generic, electronically mediated forum for human social interactions. The ways in which those interactions take place and the forms of the communities that develop depend on the *local* social needs of individuals. Such "virtual" or online communities, like communities in the "real world", are best understood and predicted through an analysis of the *metadata* that describes them. Communities are *open* or *clandestine*, according to their *purpose* (or organizing principle), *accessibility*, level of *trust*, and primary *mode of connectedness* (bonding or bridging ties). Transience and persistence are characteristics that depend upon purpose and level of trust.

Successful networkers, the "digerati" or, in the case of the military, *netwarriors* must possess the components of *network capital* (access to technology, computer literacy, and social networking ability), a strong tendency to engage in *trusting behavior*, high *cognitive ability* and some *education*. These qualities are useful not only in information warriors, but in a highly networked military in general.

If this view of cyberspace and its users is accurate, it strongly implies the need for changes in the way that the military has traditionally viewed and used CMCTs. CMCTs are above all *social* technologies. To deny their social uses is to deny the power of organized social interaction to achieve collective purposes. Virtual communities offer a mosaic of social behaviors and practices, not to mention topologies and interface methodologies that may provide models for virtual organization(s) within the military. The following chapters examine how CMCTs and the identified factors play out in actual communities on the Internet.

IV. CASE STUDY 1: *EVERQUEST* -- LOCALITY IN CYBERSPACE

> Communities are to be distinguished, not by their falsity/genuineness, but by the style in which they are imagined
>
> - Benedict Anderson; *Imagined Communities: Reflections on the Origin and Spread of Nationalism.*

A. INTRODUCTION

Most, if not all of the popular literature describing online communities at one point or another mentions MUDs (Multi User Dungeons/Domains) and/or MOOs (MUDs – Object Oriented). Most deal almost exclusively with LambdaMOO. The term "dungeon," of course, derives from the seminal multiple player role-playing game, *Dungeons and Dragons*, and describes with this allusion the character and purpose of these communities. LambdaMOO and many others like it developed before the advent of graphical user interfaces (GUIs) during the "dark" days of MS DOS and TelNET. As such, like their commercial single-player counterparts, Sierra's *Zork* trilogy of games, MUDs and MOOs are primarily text and code-based. Unlike commercial games, however, members of MUDs and MOOs have a certain stake in the virtual worlds they inhabit, for they are also its creators. A mastery of the MUD/MOO's programming language and conventions allows members to build text-based virtual edifices and fill them with virtual amenities. Certain chat communities (notably *The Palace*) permit construction of visually personalized chat rooms, and allow access to the programming language as well. Others, such as Activeworlds.com provide an interface much more like *EverQuest*, although ActiveWorlds is solely a social forum (3-D chat room with avatars). ActiveWorlds and *The Palace* straddle the line between graphics and text based communities. Among the MUDs and MOOs, the commonality of language and members' investment in "building" something naturally draws them together as communities. Systems of governance and other normative behaviors emerge, since by being able to manipulate code, expert players gain a great deal of power.

EverQuest in many ways fulfills the fondest dreams of the MUDers and MOOers because it offers an immersive, 3-D visual experience. At the same time, *EverQuest*ors do not have the same stake in the system the member-architects of the MUDs and MOOs have. However, players do become invested in the characters they construct, as many of them can relate. Losing a high-level character with many unique and hard-won skills, virtual artifacts and wealth is often a highly emotional event, although perhaps it is not so much the character that is mourned as the loss of time and effort the "deceased" character represents.

EverQuest does not represent a threat to the survival of MUDs and MOOs. Their members maintain their own culture, made distinctive by their expertise in coding, and will continue to draw those interested in constructing something of their own in cyber-space. It may be that new communities will evolve that take advantage of open source-code operating systems such as Linux to create graphical virtual realms and thus carry on the legacy of the MUDs and MOOs.

B. COMMUNITY DESCRIPTION

EverQuest is a commercially owned and regulated Massively-Multiplayer Online Role-Playing Game (MMORPG). One of the strongest attractions of *EverQuest* is the opportunity to engage in fantasy identity play, in much the same way that players of *Dungeons and Dragons* enjoy. The distinctions, however, are dramatic. Players represent themselves through photorealistic 3-D avatars that can roam throughout the virtual world of *EverQuest* (provided the player has installed the necessary files, and gained the necessary experience). Players have the opportunity to engage in conversation and collaboration with thousands of other players, and are free to form tight-knit cliques ("parties") or larger groups called "Guilds, in which members share the virtual profits (virtual currency, loot and experience) they individually gain.

EverQuest is the exemplar of what Preece calls the "virtual worlds" approach to online communities.

> Participation generally occurs regularly over long periods, of weeks or months, so there is opportunity for relationship building. Consequently,

> prolonged, repetitive interaction is seen as a criterion for an online community by participants and researchers. (Participants) think the term online community has been usurped to describe less intense social interaction such as occurs in typical bulletin boards.[38]

At the same time, *EverQuest* is also representative of what Preece calls the "E-commerce perspective."

> For them, the important issue is what draws people to and holds people in a Web site, a concept known as *stickiness*, so that they will buy goods or services. …This highly commercial perspective devalues the concept of community. But, as Steve Jones points out, the Internet, and particularly the Web, is a market driven social space.[39]

EverQuest is therefore a hybrid community that exists for one primary purpose: to earn profits for Sony Entertainment Online (SOE) and its design team at Verant Interactive by providing an engrossing virtual experience for players. The experience draws subscribing players for many reasons. For most, the world of *EverQuest* provides an escapist fantasy, with characters and a plotline to match any movie or novel, with the sticky features of being interactive and providing sociability. *EverQuest* offers several distinct interface methodologies: the primary gaming environment, and "behind the scenes" chat rooms and message boards. Beyond the game itself, a wide variety of websites and message boards (Figure 1) exist on the Web. These allow players to discuss the game, establish free e-mail accounts and web pages for guilds, and even participate in a market of sorts that allows players to sell their characters, equipment, and even *EverQuest* currency for real currency (1000 "platinum pieces" = 1 U.S. Dollar).

I find it interesting to note that in cyberspace, the social networks and systems of governance that arise model many of humanity's *older* experiments in political organization. The governing "wizards" of LambdaMOO, who are nothing so much as magistrates, returned to govern after an ill-fated experiment with democracy. Guilds in *EverQuest* resemble mafiaesque circles of trust and reputation.

---

[38] Preece. (2000). p. 16.

[39] Ibid. p. 17

1. Purpose

As stated in the preceding section, *EverQuest* exists to make money for Sony Online Entertainment and Verant Interactive. However, the purposes of its subscribers are as varied as they themselves are. Most players are there to "beat the game" and to enjoy contact with like-minded others:

> the vast majority of the interaction between players on an *EverQuest* server focuses on issues more specific to the achievement of the game's basic goals--defeating monsters, acquiring powerful or valuable items, and traversing dangerous territory [40]

A fundamental, indeed primary, object of the game is to build one's character in terms of strength, skill, power and wealth. The encouraged (and most efficient) solution for achieving this objective is for players to form groups. Players can band together into parties to collectively accomplish this purpose. Players dissatisfied with Sony's policies or Verant Interactive's management of realms and character classes often band together to suggest or demand changes. Groups of players may also form "unofficial" organizations (guilds) that operate within the game realm to advance their own status or self-esteem needs. *EverQuest* is a forum, a bundled set of interface methodologies. Unlike the worlds of the MUDs and MOOs where most players were fluent in the programming language of the game, *EverQuest*ors are vulnerable to hackers, viruses, and all the other problems that are part of existing in the global technological network. One cannot view *EverQuest* as a whole as a true community, but rather as an organizing principle and a social space that will be occupied by, and support, social groups, communities, and networks among the players.

2. Broad Accessibility

Access to *EverQuest* can be had by anyone with a powerful enough computer, a modem or broadband connection to the Internet, and a credit card. Membership in Guilds is another matter, although they too, are theoretically open to anyone.

[40] Hayot and Wesp. (2004) para. 16.

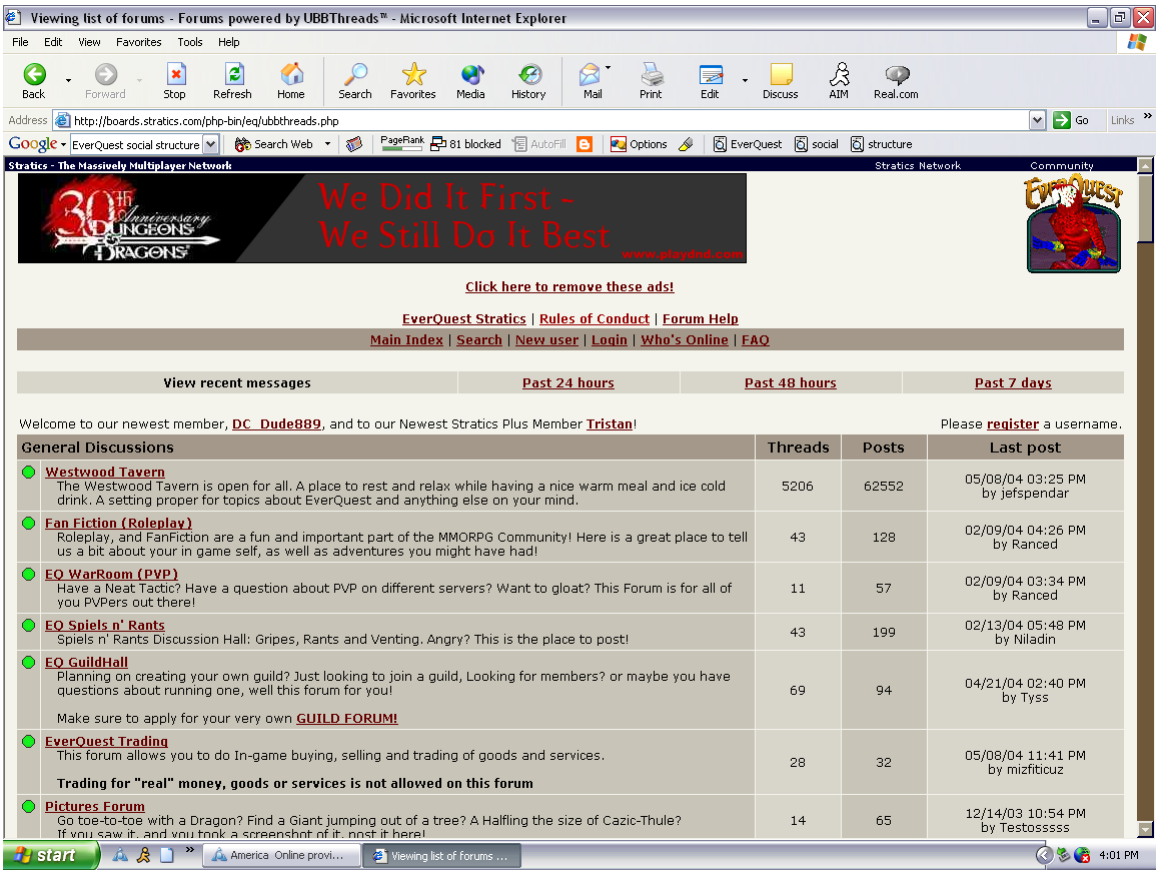


Figure 3. *EverQuest* Stratics Message Board. (Source http://boards.stratic.com/php-bin/eq/ubbthreads.php)

3. Trust

a. Trust in Technology/Network

*EverQuest*ors trust the technology enough to commit their credit card numbers and personal information to SOE. There is an expectation that the network will be there, that their favorite server will be up, and that the network is well regulated enough that hackers, viruses and other online perils will be minimized. As overheard on an *EverQuest* chat channel, “EQ has been around a long time. You don’t have to worry about hackers here like you do on other online games.”

b. Trust in Others

Most players encountered within the game world are willing to talk and to strike up acquaintanceships, and band together in parties or guilds (although this last is expected as a smart strategy for success in the game). Trust can be a fickle thing, however. Each character may or may not be acting out his or her character's behavior. It is an accepted fact among role-playing gamers that one's character is not necessarily representative of the player, although consistent behavior is expected. Trust also is embedded in the structure of the game, insofar as success depends upon cooperation.

Informal reputation systems exist to enforce trustworthiness. My observations while playing *EverQuest* tend to confirm Jakobsson and Taylor's observations about the social network among *EverQuest*ors:

> In the absence of potent enforcement of law and order, the issue of trust – not unlike what the situation in Sicily has been historically – becomes central. Alternative methods of policing, punishment and enforcement emerge. Reputation systems come to fill in an important gap left by the myriad of violations that threaten to spoil the everyday gaming experience of the EQ players[41]

The game is designed so that it is nearly impossible to succeed operating as a solo player. "Twinking" is a common practice in which more experienced and wealthy players give new players virtual money and equipment to enhance their character's capabilities and survivability. The social network is not closed, per se, but connections, trust, and reputation play a large part.

Trust within the game is of great importance. In *Dungeons and Dragons*, the game is played usually among a few friends or at least acquaintances that know each other to some degree. The anonymity granted by the Internet tends to strip away some inhibitions, and players may find themselves tempted to behave socially in ways they would not consider were all the players together in the same physical space. There are rules of etiquette to be followed in *EverQuest*. Surfing the message boards, one can find any number of postings complaining of certain players' rude behavior and

[41] Jakobsson and Taylor. (2003). p. 83.

advocating proper behavior and acceptable methods of dealing with deviants. Online Game Masters monitor activity and respond to players' concerns over others' behavior, sometimes expelling players and suspending their accounts.

Informal reputation systems exist, in which players pass information about specific characters who have behaved badly other players, thus decreasing the "bad" players' chances of success by reducing the likelihood that they will be invited to join a party, get "twinked," or otherwise enjoy the benefits of good social standing. Those passing the reputation information may do so through a variety of media including chat, posting messages, sending e-mail, instant messaging, etc. Guilds often have formal reputation systems, and their leaders have the power both to invite new members and to remove deviants. Players who have strong offline connections, family or friends already in a guild have the advantage when it comes to joining and receiving invitations to join. Guilds often bank equipment, money and spells, although the game does not support any formal guild banking system. One or several members serve as the repositories, actually holding all the items in their character's inventory. Items are releasable only to guild members, and there is an expectation that these items will be returned when no longer needed, or at least passed on to another within the guild.

4. Mode of Connectedness

The primary mode of connectedness is through bridging ties, both technologically and socially. Players log into a given server, which then relays the actions and words of each player to all others within a given radius (approximately sixty feet as measured within the game). Although all players experience the same realms, they are not *all* capable of viewing or communicating with each other. Only players logged into the same server can interact. There is a strong localizing effect because of this technical limitation.

Although the technological network is composed of bridging ties, it does support and even encourage the development of bonding ties. Players who strike up friendships and who want to maintain regular mutual contact can use the "/friend" command to add each other to their respective "friends lists." Typing "/who friends all" lets them see

which friends are logged onto their server and their locations within the game world. Guilds are especially noteworthy for their attempts to create and sustain bonding ties among their members: Abjurations to "keep it in the Guild," regarding equipment, etc.; posted rules to the effect that coordinated guild play events (raids) must be attended; guild-only chat-channels and the like abound in *EverQuest*.

5. Persistence

EverQuest has existed for several years, and continues to draw players from a wide range of backgrounds and cultures. Some writers have opined that *EverQuest* has succeeded in persisting as a *community* because Sony gave the community something to organize around, namely the game itself. Other sites designed primarily to facilitate sociability have failed precisely because there was no specific organizing principle. While this is a significant factor in explaining the game's longevity, it also has to do with the way social values are encoded in the structure of the game itself, and in the social networks that develop within the context of the game.

Repeat participation (player persistence) is often a qualification for membership in assorted Guilds, where the good of the group is expected to outweigh members' prerogatives. Assorted guild websites, bulletin boards and guild members themselves relay various formulations of this rule. Continued membership in the guild often depends on a player's reputation for teamwork.

Hayot and Wesp advance the idea that *EverQuest* persists because of a structurally encoded tension between opposing forces: *community*, driven by the need to cooperate to succeed, and *alienation*, caused by the fact that game time continues on even when a given user is logged out (the player then misses events and opportunities to advance with peers).

> This opposition or bind between alienation and community is the central effect of the game elements on the players' experience of *EverQuest*; that is, the relation between these two fundamental structures in the game establishes, dialectically, both the reason to avoid playing the game (the alienating, temporal vastness of unheroic indifference) and the reason that

the game is so compelling to play (the opportunity to overcome that vastness and indifference through community formation)[42]

Brad McQuaid, one of the designers of *EverQuest* put it a different way:

> Community is relationships between players …It's also a form of *persistence*, which is key to massively multiplayer games. Without community, you simply have a bunch of independent players running around the same environment. Players won't be drawn in and there won't be anything there to bind them. The key to creating community, therefore, is interdependence. … By creating an environment often too challenging for a solo player, people are compelled to group and even to form large guilds and alliances. All of this builds community, and it all keeps players coming back for more and more.[43]

6. Interface Methodology

The user interface is complex; to list all controls and functions here would be impractical. (The user manual is approximately 162 pages long). However, a short description should convey the feel of the game: One is presented with a first-person perspective of the immediate environment, which forms the background of the interface window. Layered atop this depiction are the player's control windows, which include the Main Chat window and a "Window Selector" toolbar, which opens various windows (Actions, Inventory, Options, Friends, Hotbuttons, Spells, Pet, Effects, Songs, Guild Manager, Map, Storyline, Journal, and Help). Each of these windows contains buttons to open sub-windows. For example, opening the Actions window presents the player with several tabs: "Main" (most common actions), "Skills," "Combat Skills," and "Socials." The Socials tab may be programmed with various commands such as "/wave," "/say (insert phrase)," and "/invite" (invites other players to join your party) for quick use. Other characters (player and non-player) as well as various enemies display labels above their avatar. (See Figure 3.) Guild members often display their guild affiliation with a second line below their character's name, called a "guild-tag."

[42] Hayot and Wesp. (2004). para. 39.

[43] Aihoshi. (27 Sep 2000). Emphasis mine.

C. MEMBERS

EverQuest would not exist without computer-mediated communications technologies. No broad studies of the demographics of *EverQuest* players have been conducted, although some data indicates that *EverQuest*ors represent a broad sample of the general population. Because *EverQuest* is what it is, some assumptions may be made about its membership, in terms of network capital, wealth and education, and cognitive ability.

Figure 4. The *EverQuest* User Interface (Source: http://eqlive.station.sony.com/interface/.)

1. Network Capital

a. Access to Computers

If one is playing *EverQuest*, by definition, one has access to a computer and the Internet. Demographically speaking, this means that those playing *EverQuest* are likely to be in the middle-income bracket or above.

b. Technological Literacy

If one is playing *EverQuest*, one must be familiar with the operation of their computer and have the ability to use it to connect to the Internet. In addition to having some degree of competence with the computer interface itself, the complexity of the game's interface methodology requires a certain technical skill as well.

EverQuest players may be assumed, then, to possess the first two elements of network capital, access and literacy.

c. Social Networking Ability– Locality and Guilds

EverQuest demonstrates the local nature of cyberspace in both its technological arrangement and the ways groups tend to socialize. The rules of the forum dictate the limits on socialization, but the predominant social form of *EverQuest*, the "Guild", is hardly new, and very human.

> The production of social networks and the circulation of social capital *(here meaning goods held in common)* proves to be one of the most important aspects in EQ. …On the one hand extreme benefits are accrued through the social connections and knowledge this structure provides. Yet the sense that some remain either locked in or locked out of the *right* connections lingers.[44]

As Hayot and Wesp point out, the need of players to band together is a near requirement of the game. This banding together often crosses national boundaries in the real world, yet the perspective of each player is always local. Use of the term *local* here recalls the definition from Chapter II, with its three dimensions: spatial, temporal, and contextual.

[44] Jakobsson and Taylor. (2003). p.88 Parenthetical mine.

Spatial locality in *EverQuest* results from the geographic nature of the virtual space that is the game world, and from the technical connectedness of the network of servers. The virtual world of *EverQuest* (called Norrath) is divided into five continents, Norrath's moon is also inhabited, and there are the realms of the elements and of the various fictional deities of Norrath. New characters begin in whatever region their character's race inhabits, and find it difficult to leave their "homeland" until they have gained some experience (and probably joined or formed a party). Moreover, although there may be up to 144,000 players online at any given moment, they are divided between 48 servers (3,000 per server). Players can only interact with players who are logged into the same server; moreover, cooperative behavior (within the game) can only occur among players who are collocated in the same virtual sixty-foot space.[45] Guilds therefore tend to organize on given servers. The characters and reputations of the guilds vary from server to server.

Temporal locality in *EverQuest* is a function of the ways characters progress. All characters begin at a basic skill Level (1), with a minimum load-out of equipment and almost no money. Advancement is entirely up to the player. Because players can log out at any time and remain out of the game as long as they wish, vast differences in skill, power, equipment, and wealth can arise between players who essentially started simultaneously. Time and participation are the main determinants of advancement. According to one player, this creates a

> basic vertical social stratification caused by different character levels (someone with a level 5 main character is *highly unlikely to associate with someone with a 65*, unless the owner of the 65 is playing a level 5 alt(ernative character). This is a little more complicated than just comparing levels; particularly at the top end you have a wide gap in equipment/skills/experience between the folks who have been level 65 for a week, and those who have been playing for five years[46]

Turning again to Hayot and Wesp:

[45] Hayot and Wesp. (2004) para. 14. Also para 20: "As a result of the game's efforts to enforce these geographic limitations, players cannot help but encounter and become familiar early on with characters of their own race near their 'home' town, thereby encouraging from the beginning of the player's experience a sense of locality and distinction within an online community of players defined by its vastness."

[46] E-mail correspondence from "Chris" dated 28 April 2004.

> The drive towards balance and homogeneity means that the only distinction between any two characters in *EverQuest* can be understood simply as a difference in *time.* Because of balance, the external limiting factor on a character's success is the amount of time it is played: today's brand-new character can, within a year or so, be as powerful as any other character.[47]

Two types of guilds exist in Norrath; "überplayer" guilds and social guilds, the difference between them is that the *über*guilds focus on game play and achievement whereas the social guilds focus on, well, socializing. Both types comprise certain social strata, based on character skill level, which is based, as we have seen, on time spent playing. Truly, temporal locality determines a player's social standing and peer group.

Contextual locality is the culture of the game itself as well as the pre-existing social networks of the players. Players who form parties, guilds, post messages and otherwise participate in the multiple forums associated with *EverQuest* are embedded in a system of meaning, values and behaviors that are strongly associated with playing the game, yet they do not relinquish their prior social identity even when online, but rather tend to maintain it. The fictional histories and quest descriptions that are a part of the game shape the language of players, and provide convenient ways for insiders to identify outsiders, but do not in any real way describe the people or social groupings within the culture of the game. Instead, it is the formation and behavior of Guilds that most characterizes the game culture. For example:

> By being a member of certain 'Guilds' you are automatically given a certain stigma. Such as there is a guild known as the King's Armada. If you are a member of this group, then many people will not like you or even group with you because this 'Guild' while large is not well liked (*sic)* [48]

Membership in a guild is often the key attribute that facilitates "twinking" and thus more rapid advancement. Upon creating a new character, that character is granted membership in the "guild" associated with their character's class (their vocation: warrior, enchanter, ranger, cleric, etc.). These guilds are part of the "given" world of the game, and serve generally the same function that trade guilds perform – training.

[47] Hayot and Wesp. (2004) para. 29.

[48] E-mail correspondence from "Chris", dated 5 May 2004.

Player-created guilds, while officially sanctioned, are not necessarily run by SOE/VI, and may end-run other technical and social boundaries, crosscutting servers, nationality, and experience levels. Guilds can and do assume a group identity, although as the player quoted above points out, perceptions of members and perceptions of outsiders can differ greatly. Often, player guilds have their own web sites, message boards, and chat rooms that exist separately from the official forums and chats hosted by SOE.

At the same time, players more often than not maintain and even reinforce their pre-existing social affiliations.

> Totaly separate to guilds, players tend to associate with other players who hang out in the same chat channel, which is usually based on a separate theme - for example I'm usually in the Australian chat channel on my server, and am likely to communicate with and/or group with other australians. …Everquest players seem to be a very broad slice of the international community - a fact you might not pick up unless you post to places where the french, german and japanese players might read and reply (s*ic*).[49]

Social networking ability as defined in this study (the ability of the individual to internalize and act upon the metadata that describes the social network in which he or she is embedded) is the ultimate determinant of a player's ultimate success in EverQuest. High-level players must posses a modicum of it, and those who rise to leadership positions with the Guilds must have even more. *EverQuest* enforces a sense of locality: Locality of character class, of geographic origin and character race, of experience and peer group, as well as locality of server. However, players maintain their offline affiliations as well. Family members and real-lie friends tend to group together, as do various real-world nationalities.

> Certainly *EverQuest* players experience their communities transnationally and outside *traditional* forms of the local…. But as we have shown, the political forms suggested by the game's complex register of time and space are, for all that, *not necessarily different than ones we already know*. …That is, though the communities *EverQuest* forms (or encourages play-

[49] E-mail correspondence from "John", dated 5 May 2004.

> ers to conceive and form) may well be 'new,' the difference that newness makes may simply be a difference we already know.[50]

No evidence of infiltration or overt inter-guild warfare was evident in the course of this study, although the possibility certainly exists. Further studies of social warfare among *EverQuest*ors, if it exists, could prove to be very enlightening.

2. Cognitive Skills and Education

Despite the fact that no conclusive demographic studies of *EverQuest*ors have been conducted, their ability to access computer networks and to use them effectively to achieve their purposes, especially in view of the complex user interface and broad range of forums associated with the global *EverQuest* community, indicates that these people are of generally higher than average intelligence and cognitive ability. Although my discussions with other players have been too limited to be statistically significant, they tend to compare with the findings of the UCLA study discussed in Chapter III.[51]

D. CONCLUSION

Although *EverQuest*, as a whole, does not constitute a community, it is both an organizing principle and a social space in and around which communities develop. These communities demonstrate the basic characteristics of open communities as examined in Chapter III, as well as the characteristics predicted for its members.

The fact that the larger community of *EverQuest* players must be familiar with the use of multiple interface methodologies is of interest. Traditionally, virtual ethnographers have looked at communities as bounded by the nature of their interface methodologies. Clearly, virtual communities can extend far beyond a single interface method.

[50] Hayot and Wesp. (2004). para. 43-45. Emphasis mine.

[51] Two examples: Chris "I am 21 years old, I work in a retail food store (Albertsons), I am a US citizen, I have been working with computers for about 13 years now. I have been playing EverQuest for about 3 years now. I started it to hopefully have a game that I could spend ($) 13/mo on instead of spending ($) 50/mo on different games that I would have beaten inside of a week. Also, EverQuest gave me something I was not expecting: it gave me friends. I feel a unique bond to these people even though I have never met them, I know that they care for me and they have helped me through many difficult times in my life," and John: "Education: High School; Profession: IT systems administrator; Nationality: Australian; Approx age: 27, Computers: 19 years, Internet: 8 years." (E-mail correspondence; parentheticals in Chris's statement mine).

Information Operators in the military must be able to move between interface methodologies and recognize the existence of communities that transcend interface methods. Al Qa'ida is another community based around a common activity and/or organizing principle, as we shall see.

For the intelligence community, its primary reliance on e-mail and web pages is an intensely limiting factor. This particular method is overly centralized, and all too often reinforces intra-agency boundaries and "fiefdoms" at the expense of the smooth and timely flow of information. Local intelligence shops have local perspectives and local needs, yet the community is organized in a rigidly compartmented, hierarchical fashion that does not permit rapid sharing and dissemination of tailored information, and does not take advantage of the wide variety of communications methodologies afforded by CMCTs. Having pointed out these problems, it remains to provide recommendations for their solution. Before proceeding to do so, it will be necessary to examine a few more communities to fully appreciate how the potential of CMCTs is being underutilized, mismanaged, and even abused in the military community.

V. CASE STUDY 2: AMERICA ONLINE CHAT -- PURPOSE AND PERSISTENCE

A. INTRODUCTION

Hamman calls America Online (AOL) a "city in cyberspace," because of the vast array of activities possible there: Online shopping, research, travel planning, investing, advice, listening to music, classified advertising including personals, a dating service, e-mail, message boards and newsgroups, and of course, chat rooms. If communities can be distinguished by interface methodology and purpose, the larger AOL "community" can be subdivided into many distinct groups just as the population of a city can be broken down into distinct groups.

Except for e-mail, chat rooms are the most common service used by AOL subscribers. The question, of course, is do chartroom participants form communities? A quick look at the types of AOL chats available indicates that there is some support for this hypothesis. Chat rooms exist to serve almost every kind of community that can be described. There are sectarian chats, gay and lesbian chats, age-based chats, film and music genre chats, geographically based chats, chats for expectant parents and parents of toddlers to teens, even a military chat. The problem, however, is that while all of these chats are available, there is a very high turnover rate. While some members return to the same chats repeatedly, many do not. The issue of persistence with regard to chats is an important one. While the AOL-created forums may persist, the body of members chatting in any given room varies considerably over time. In many cases, long-time members may not even participate in the general forum, preferring instead to use AOL's instant messaging service to communicate with a relatively small circle of friends, a practice known as "lofting." Some chartroom participants are outspoken against lofting, but the practice is very widespread.

Moreover, as Hamman points out,

> many AOL users are motivated to join the online service to conduct research and to communicate via computer with people they already know

> offline rather than to meet new people online and to build new friendships with them. … This stands in opposition to a number of theorists and researchers who have written that computer mediated communication (CMC) can lead to the disintegration of pre-existing communities.[52]

For the purposes of this study, I participated in two chats; one in an AOL-created forum, the other an informal group that rarely met in the same named chat room more than once. The reason for this was to see if there were any differences between the communities formed in persistent forums, and ad-hoc forums. As it turns out, among AOL chat room participants, social bonds exist independently of forum. Although social bonds do develop, at least in my experience, the bonds were too weak to facilitate long-term contacts, or (in the case of the informal group) even to maintain the existence of the group for longer than a few months. Jennifer Preece and fellow researchers claim community lifespan is a factor affecting the closeness felt among its members[53]. I argue that community lifespan is a dependent, rather than an independent variable. The lifespan of any community depends upon the strength of the bonds holding it together, which depends upon the sustained common interests and purpose shared by its members.

While AOL chat groups, as such, cannot be considered models for military organizations of any stripe, they do offer a model of sociability that is altogether lacking in DoD networks. As we become more reliant on computer networks to do our jobs, it has become more and more necessary for units to stage formal formations, mandatory commanders' calls, and off-site events to restore and maintain the sense of camaraderie and unit cohesion that often has been the hallmark of membership in a military organization. This is not the fault of the technology, but rather the result of a parsimonious conservation of bandwidth and a misapprehension of the nature and value of social technologies such as chat rooms and instant messaging (IM).

Experiments are underway in the intelligence community to find the means to achieve real-time, cross-speciality conferencing, or in the words of the Advanced Analy-

---

[52] Hamman. (1999).

[53] Preece, et al. (2003).

sis Laboratory of the National Security Agency's "Call for Advanced Capabilities for Intelligence Analysis", "heterogeneous collaboration":

> Recent experiments suggest that most collaboration takes place in the domain of *discourse shared by analysts*, not in the disparate worlds of specialized, unique knowledge that each analyst might possess. Collaboration thus takes place within the intersection, not the union, of the knowledge sets that analysts bring to the table.

The attempts to formalize and implement collaboration systems in USCENTCOM's J2 division that I witnessed were not particularly successful. The use of common commercially available software for implementing chat forums and IMs in a protected domain/multi-level system environment, with rigorous auditing, could ensure that analysts in different areas could collaborate from their desktops easily, and within their security classification and compartments.

B. COMMUNITY DESCRIPTION

According to Hamman

> AOL is … 'a community' that has many aspects of a physical community. These aspects of community include the use of group specific language, a virtual *proximity* to other members of the community and, in some cases, a common purpose for using online technologies.[54]

However, because AOL is so extensive and encapsulates so many disparate groups, it makes little sense to talk about an AOL "community" because ultimately, subscribers share only the access methodology (the AOL software) and some common terminology.

As stated in the Introduction, I participated in two chat groups. The first was the "Thirty Something" chat; an AOL-created chat room (as opposed to a member-created room). Ostensibly, the Thirty Something room is a forum for people of a certain age to get together and socialize. The majority of participants did not invest themselves in the chat room, since the membership changed continuously. The chat was not exceptionally different from a majority of other chat rooms, in that conversation within the room

[54] Hamman. (30 Sep 96).

tended to consist of participants greeting each other and requesting “age/sex/location” checks periodically. Members who knew each other often became inactive in the main chat -- not because they were lurking, but because they were lofting. It must be noted here that finding partners for the purpose of having “cybersex” with them seems to occupy a great deal of chat participants’ time. Often, when the seekers make contact, either they will do their thing via IM, or they will create a private chat room.

The other chat group had no formal name, although members tended to know each other in the traditional social networking sense discussed throughout this paper. I call this the “Wolf Group,” since the common feature among members was a penchant for including wolf-related terminology in their screennames, such as “SlverAngelWolf,” or “AmaroksFangs.” The Wolf Group engaged in a sort of fantasy role-playing where members pretended to be either actual wolves or werewolves and interacted as such, although “staying in character” was not a consistent behavior. More often than not, the membership appeared drawn from a larger body of role-playing gamers who used the room as a casual break from their other games. The trick to finding each other was to use AOL’s “BuddyList” feature, which allows subscribers to keep track of their contacts who are online.

Figure 5. AOL Chat Selection Screen (Screenshot).

The "Locate AOL Member Online" function allows members to find the chat room location of their friends so that they, too, can enter that chat room. One may also use the AOL Chat Room Listings screen (Figure 4) to search available chats by type (AOL or member-created), theme ("Life," "Romance," "Places") and chat room name, or by topic keyword. The "Who's Chatting Button" allows the user to see the screennames – and personal profile – of everyone participating in the room. In this way, any Wolf Group member could create a chat room and eventually, the other members would find their way in. Even when the member who created the room left, the other members would keep the room open for hours.

1. Purpose

Hamman's research suggests that AOL members subscribe to the service in order to maintain their pre-existing social networks, rather than to form new communities. While this may be their primary motivation in subscribing to AOL, members can be quite open to forming new relationships online. Purpose in AOL chat rooms is entirely de-

pendent on individual members' interests. Often, the primary purpose appears to be the quest for cybersex partners, idle flirtation, or overcoming boredom.

Unlike *EverQuest*, in which there is a common purpose among all players, AOL Chat offers no common purpose. For this reason, AOL chat "communities" have varying life spans. Infrequently, several members who have never met offline develop intense personal friendships that transcend the technology. To characterize relationships such as these would be difficult. In the group I was privileged to witness, each of these people had problems in their real lives and was able to find emotional support and validation from each other. The intensity of their relationships was undoubtedly influenced by these factors. However, the relatively small size of these groups prevents them from being true communities.

Malcolm Gladwell, citing research by anthropologist Robin Dunbar, suggests there is a "magic number" of participants (about 150) above which communities cannot continue to exist as communities, and which is based on the average number of social connections the human brain can keep track of at any given time (social channel capacity).[55] Persistent face–to-face interaction within groups tends to reinforce these bonds, strengthening them. Many theorists have opposed the idea that communities cannot truly exist online, because the face-to-face element does not exist. However, I argue that communities can exist online, even in the absence of face-to-face interaction, if there is a common purpose and a personal commitment on the part of each member.

AOL chat, however, lacks both fundamental characteristics that would tend to support the development of true communities. First, while chat rooms generally do not exceed thirty-three participants at any one time, the turnover rate (members joining and leaving) requires participants to keep track of far more than 150 others in the course of a session. Second, the lack of either common purpose or face-to-face interaction inhibits the formation of community. Relatively large groups can form around a common interest, but they persist only so long as the membership maintains the common interest in participating with each other. Persistent groups in AOL chat rooms tend to be small (generally fewer then thirty, and most often less than five), reflecting the broader struc-

[55] Gladwell. (2002). pp. 177-181

tural lack of support to community development. Participants may have feeling that they are part of a "community," yet it is at best a nebulous and ill-defined sense. When participants speak of the "30's" chat community, they tend to refer to a *few* persistent contacts whom they met initially in the chat room and who tend to be there with some regularity.

2. Broad Accessibility

AOL is accessible to anyone with a communications device and the ability to pay for the service. AOL members can access their e-mail, surf the web, chat or IM from any number of devices including computers, wireless equipped PDAs, and cell phones.

3. Trust

AOL enforces certain rules, called "Terms of Service" (TOS), that generally govern offensive behavior in its chat rooms, message boards, and newsgroups. There are volunteer monitors who police chats, news groups and postings. AOL monitors can bar violators from further access to AOL. This strict enforcement mechanism against deviant behavior enhances the level of trust AOL members have in the service and in their fellow members.

In chat rooms, however, there is a lower level of trust, reflected in the unofficial norms that govern chat room behavior. One example is the requirement that participants who expect interaction must create a personal profile. Often, profiles contain explicit statements to would-be readers that the profile's owner does not appreciate unsolicited IMs, or conversely, that the reader wanting to know more should contact the owner. Females seem most likely to post injunctions against unsolicited communication in their profiles. Below are a couple of examples:

Name: that is personal
Location: USA
Gender: Female
Marital Status: SINGLE
Hobbies & Interests: ASK ME

Favorite Gadgets: none
Personal Quote: I dont have a quote DO NOT IM ME IF YOU ARE MARRIED

Name: **Lord**
Location: **My Den**
Gender: **Male**
Marital Status: **owner of a broken heart**
Hobbies & Interests: **hunting,fishing,an looking at pics of Dragons**
Favorite Gadgets: **Breathing Fire**
Occupation: **Guarding my Den**
Personal Quote: **do not medle in the affairs of Dragons because your crunchy an taste good with ketchup**

Name: This is the important part: DO NOT IM ME WITH A/S/L!
Location: Chicago burb
Gender: Female
Marital Status: Divorced w/a litter
Personal Quote: If you have nothing nice to say, come sit next to me! :X…..AND No profile, No pic, NO CHAT…..Also, isn't nice to steal others quotes as "your own". :)

Many AOL chat members also post personal web pages, a practice that AOL facilitates and encourages in its efforts to build community with pre-built templates and links. Member web pages often serve as an expansion of the member's profile, and represent deliberate acts of evocative trust, as well as more generalized trusting behavior.

4. Mode of Connectedness

Weak or bridging ties are by far the most prevalent form of connection among AOL chat participants. Although AOL makes efforts to build community by facilitating and encouraging trusting behavior, such as the use of profiles and personal web sites, and members often exchange photos of each other in attempts to overcome the lack of face-to-face communication, strong (boding) ties are rare, and generally limited to members of small groups or cliques.

5. Persistence

Persistence in AOL chat groups is unrelated to any specific forum. While some chat rooms like “Thirty Something” possess persistence, they are not true communities by our definition because they are not discreet groups of identifiable people interacting with anything resembling regularity. On the other hand, one might consider the Wolf Group a community because although they used transient forums, there was a persistent (if weak) sense of group identity. The Wolf Group, however, had a definite lifespan. Within about four months of joining the group, it became increasingly difficult to locate wolf-related chat rooms, and members began changing their screen names or canceling their subscriptions to AOL so that eventually none could be found and the group had ceased to exist.

The primary reason for the short life spans exhibited by groups that form in AOL chat has to do with the lack of a strong common purpose. Without a common purpose, members are not committed to the group, and their participation continues only so long as it holds their interest. A strong critique of the idea of online communities has always been the ease with which members may disengage from the group. As seen in the EverQuest case study, EverQuest guilds have strong community norms concerning regular participation, and social enforcement mechanisms that encourage consistent participation. AOL chats, beyond the official TOS rules about obscene, rude, or threatening behavior, have only weak norms governing interaction.

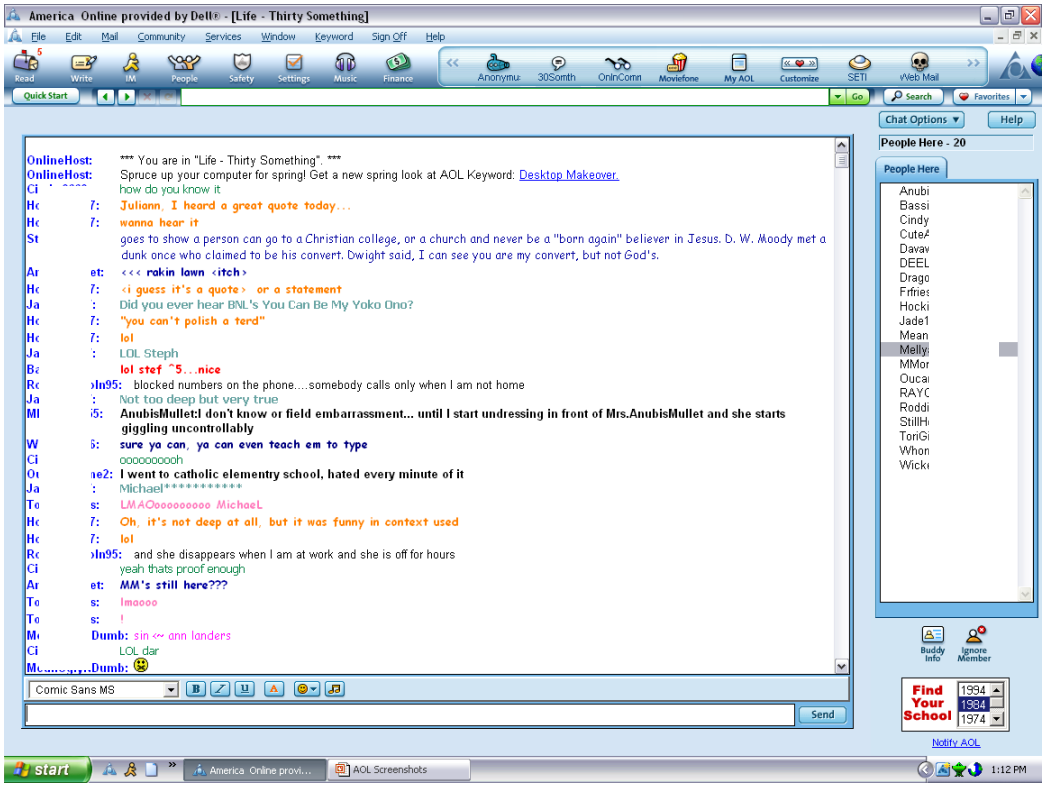


Figure 6. AOL "Thirty Something" Chat Room (Screenshot)

C. MEMBERS

1. Network Capital

Most AOL members are not "digerati." They may possess some or all of the attributes that constitute network capital; however, they are as the UCLA study found, ordinary people who have chosen to include cyberspace as one of several forums for interaction, and perhaps not even their primary venue for social interaction.

a. Access to Technology

As was the case with *EverQuest*, membership in AOL presupposes access to technology. The main difference is that *EverQuest* can only be played through a personal computer (Internet connected desktop or laptop) or the Sony Playstation2

game console with online adapter installed. Any stationary or mobile computing or communications device, however, can access AOL, including PDAs and cell phones.

b. Computer Literacy

The question of computer literacy has mainly to do with users' skill at using CMCT. Generally, the more interface methodologies one can use, the higher one's computer literacy. Simultaneously, the more one understands the technology itself, the higher one's computer literacy. In text-based cyberspace, there is a third dimension of computer literacy, which has to do with the use of language. Per Hamman;

> Although most online communication is done in American English, there are certain grammatical and vocabulary differences between the language used online and that used in the everyday world. Grammatical, capitalisation, and spelling errors are not only acceptable; they are expected in online communication. This is because online communicators place a higher value on rapidly conveying their point than they do on correct spelling and grammar. …People online don't write to each other in real time, they have conversations where each participant takes turns 'talking' and 'listening.'[56]

The ability to use several types of software, keep track of multiple conversational threads and manipulate multiple windows is necessary when engaged in intense chat sessions. This particular ability also speaks to the participants' cognitive abilities as well, although perversely, the ability to use software to manage multi-thread conversations may indicate slower cognitive processing than one who can manage multi-thread conversations without software assistance.

c. Social Networking Ability

Most AOL members are not adept at social networking, because they do not engage in it. Social networking, as we have seen, tends to involve a persistence and purpose in the community. In *EverQuest*, knowing the right people and involving oneself with others is necessary to the purpose for which the game exists. AOL chats exist for no purpose other than to provide a forum for interaction.

[56] Hamman. (30 Sep 96)

Some members may express a sense of community:

> I have alot of good ppl that I truly care about online. My best online buddy would have to be _____, but the whole gang from 30's each and everyone of them have good things about them. I hop from one 30's room to another but,you can catch me mostly in 30's but if i am not there you can't catch me anywhere. I am addicted to Pogo too :oP (*sic*)

However, community in the definitional sense does not exist on AOL. Members such as the one quoted above tend to socialize within a very limited circle of friends, and as Gladwell asserts, realistically cannot "know" the entire body of chat participants.

2. Trusting Behavior

Participants in AOL chats are notorious for refusing to converse with others who do not post an online "profile" associated with their screen name. The assumption is that individuals who are unwilling to front a limited amount of personal information are untrustworthy, a classic case of Sztompka's evocative trust.

As is the case in other communities, notably *EverQuest*, regular participation is a key to trustworthiness – at least in the Wolf Group. Other members of the Thirty Something group relayed their experience a bit differently than I experienced the group. One member related the fact that she had several online friends, two of whom she considered close. These friends devised unique screen names for themselves known only to each other, as well as creating "tags." Tags are images containing the screen name or given name of the participant that they insert into all outgoing e-mails. Tags served less as an indicator of authenticity, and more as a bonding activity between the members of the clique.

Figure 7. Circle of Friends "Tag." (Name blurred by request.)

The clique sought each other out online, participated in the Thirty Something chat room regularly, and established contact with others who would then return to the chat room, creating a sense of community within the otherwise unstable chat environment. The trust established within this group had a great deal to do with regularity of participation, as well as the exchange of "trust tokens" such as web pages, personal photographs and anecdotes that along with the profile of the member served to create an "authentic" identity that could then be trusted.

This particular group often participated together in chats occurring on other online services, including MSN and Yahoo. These three friends were able to maintain their bonding ties completely over the Internet, and their social connections existed independently of any named forum or service. The experience of these participants in the Thirty Something chat mirrors my experiences in the Wolf Group. The lesson here is that community depends more upon its purpose and the people who compose it, and much less on the particular interface methodology supporting it.

3. Cognitive Ability

Maintaining the thread of a conversation is simple if one is engaged in a chat or IM with only one other member. Most AOL chats, however, host as many as thirty-three

participants do. Chat participants quickly become adept at following several conversational threads, and learn to preface their remarks with the screen name or first name (if known) of the person they wish to address. Acronyms abound, and many researchers have documented them. Acceptable "chat-speak" morphs over time. The acronyms and abbreviations that were acceptable in 1994, when I first began chatting have changed with time. During a recent session, I typed "afk" meaning "away from keyboard." Upon returning, several responses appeared, members either confused as to the meaning of the acronym, or commenting negatively on the recency with which I had participated in chat rooms.

Because of the number of separate conversational threads that one can engage in (chat window plus multiple IM windows), some entrepreneurial companies market software, such as WavMan, that helps to organize the environment. WavMan allows the user to consolidate all IM windows in one indexed window. If one is away from the keyboard for extended periods, WavMan offers the ability to log the ongoing chat. In a way, logged chats offer some of the same advantages that message boards allow, in that there is a persistent record of the conversation that one can reference when authenticity or non-repudiation becomes an issue. The consummate chat participant is therefore capable not only of keeping track of several conversational threads, but of managing the interface to reduce confusion.

4. Education

No researchers have conducted comprehensive demographic surveys of the more than 14 million AOL subscribers. The majority of those I interacted with had at least a high-school education, were in college, or had some college education. Several were unemployed (at least for the time being). This contrasts sharply with Howard Rheingold's experience with the WELL (Whole Earth 'Lectronic Link), as related in his books The Virtual Community: Homesteading on the Electronic Frontier, (2000. MIT Press) and Smart Mobs: The Next Social Revolution (2002. Perseus Publishing). Rheingold's fellow members of the WELL seem to be largely older, educated, professional types. Although, as Dorothy Denning points out,

> the WELL is hard to compare with AOL because it was older and the technology was harder to use (no graphical user interface that I recall). It required more skill. It began with well educated users and spread by word of mouth, not advertising.[57]

Nevertheless, the findings of the UCLA study seem to hold true for AOL subscribers as well as *EverQuest*ors.

D. CONCLUSION

Clearly, the absence or presence of collective purpose influences the existence of community, as we have defined it. Nevertheless as Hamman makes clear, in *pre-existing communities*, chat and IM functions can serve as technological mechanisms to strengthen social bonds.

As a former member of a geographically dispersed squadron, chat/IM software implementation over the squadron intranet could have done a great deal to help unify the squadron by overcoming the physical distances and making the rest of the squadron more proximate to each member. Instead, most installations have forbidden chats and IMs, leaving only one rapid method of asynchronous communication open – e-mail. From experience, e-mail server failure generally means a degradation of productivity. The e-mail server itself becomes a single point of failure. Chat and IM software resident on clients can still be active, even if the email server goes down, providing an additional channel of redundancy.

Hamman's research suggests that the availability of chat and Instant messaging technology do not damage the integrity of participants' pre-existing communities. The fact that the military unit is a pre-existing social unit, generally conforming to Gladwell's "Law of 150," means that chat and IM services can help reinforce moral and unit identity, as well as fostering and enhancing lateral communications among mutually supporting units. As long as clear policies are established and enforced, there should be no reason the military should continue to resist the use of chat and IM functions within its networks.

[57] Personal correspondence dated 3 June 2004.

The military is a distinctive type of organization, however, and security requirements exist in spite of generally high trust among military members. Other communities online place a premium on security; those we have labelled clandestine communities. The next two case studies examine two such communities with an eye toward traits useful both for targeting and for emulation.

VI. CASE STUDY 3: PEDOPHILES ON THE NET

> *Never before have pedophiles had the opportunity to communicate so freely and directly with each other as they do online.* Their communication on the Internet provides validation, or virtual validation, for their behavior. They share their conquests, real and imagined. They discuss ways to contact and lure children online and exchange tips on seduction techniques. They are using the technology of the Internet to train and encourage each other to act out sexually with children. The Internet also serves as a tool for predators to exchange tips on the avoidance of law enforcement detection.
>
> Donna Hughes (2001)
> http://www.protectkids.com/dangers/onlinepred.htm

A. INTRODUCTION: "OPERATION CANDYMAN"

In January of 2001, FBI Houston initiated an investigation after an undercover agent identified three online communities involved in posting, exchanging and transmitting child pornography. Because of the name of the primary group, http://www.egroups.com/ groups/thecandyman, the FBI called the investigation "Operation Candyman." According to FBI statistics, published on the Web at http://www.fbi.gov/pressrel/candyman/ candymanhome.htm, the Bureau estimated there were over 7,000 members of the Candyman community, with some 2,400 residing in foreign countries. At least one subject was located in every FBI field office's territory with some field offices having up to 45 targets within their respective territories.

However, the FBI grossly misunderstood the nature of the e-group communities they had targeted. These online communities had an e-mail policy that allowed participants to automatically download *all* e-mails sent within their e-group for later perusal, or to selectively download the e-mails they wanted to view. As a result, thousands of members unwittingly downloaded child pornography. When the FBI subpoenaed members' records from Yahoo, these members found themselves charged with possession of child pornography. Because of the embarrassing nature of the charges, and the strength of the evidence (they actually had downloaded prohibited material), many of these members made plea agreements. The FBI's mistake is a testament to how poorly

online communities are understood, and how strongly interface methodology and associated policies can generate unintentional behavior.[58]

B. COMMUNITY DESCRIPTION

Before we can understand the status of online pedophiles as a community, it is necessary to look at their history just before the advent of widespread Internet access.[59] Before the Internet allowed web pages, chat rooms, and peer-to-peer networking, pedophiles had several well-known organizations that sought to provide a sense of community and mutual support among themselves. The North American Man-Boy Love Association (NAMBLA), the René Guyon Society, and the Wonderland Society were some of the more well known. These groups engaged in political activity in numerous attempts to change the laws concerning their sexual preferences; specific efforts to lower the legal age of consent predominated. These activities were carried out by anywhere from five to fifteen core members. Rank-and-file pederasts, however, carried out their activities clandestinely, relying on a social network of connections to meet and trade material. Often, these individuals had to enter neighborhoods and other areas in which their physical safety was threatened, or their identities compromised. Moreover, as the law enforcement community increased its use of covert infiltration and sting operations, meeting at all became a high-risk endeavor.

When the first electronic bulletin board systems came online, they provided a relatively much safer forum for pedophiles to communicate and exchange information and even digitized photos (slow transmission speeds often meant that uploading or

[58] Technology has facilitated the sharing of electronic images, but it has also produced some interesting legal situations. In Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002), the Supreme Court declared certain provisions of the Child Pornography Prevention Act unconstitutional to the extent that they defined child pornography by reference to images that appear to depict, or convey the impression that they depict, minors [18 U.S.C. 2256(8)(B),(D)]. As a result of this ruling, the government has an affirmative burden to prove, as an element of its case, that the images were produced using real children. According to the Department of Justice (DOJ), where a defendant claims that technology currently exists to create photo-realistic computer-generated images that appear to depict real children, it is more challenging for the government to meet its burden of proof. DOJ states that one manner of meeting that burden is to identify the child depicted in the image, which may be facilitated through the Victim Identification Program.

[59] Dr./Major Nate Galbreath, USAF, at Andrews Air Force Base provided the history of pedophilia as it appears here. Dr. Galbraith is a resident psychiatrist and former Air Force Office of Special Investigations (AFOSI) special agent. Most of his career has been involved with investigating pedophiles.

downloading a single picture often took hours). Websites and higher transmission rates allowed better security as well as increased efficiency. Webmasters and administrators restricted access to these websites, in keeping with the clandestine social networks that preceded them. One negotiated membership through social contacts and word of mouth, with existing members vouching for those who wished to join. Policies similar to current file sharing policies were enforced – membership carried with it a requirement to upload material. The policy served two purposes: to increase the amount and variety of material available to members, and to ensure loyalty. The rest of the group then knew members who uploaded material to be guilty of criminal acts; their self-interest in preserving their freedom and reputation ensured their silence about the group. Eventually, pedophiles could obtain access commercially, with members paying for access and downloads with their credit cards

Beginning in the early 1990's, however, as more and more people began to use the Internet and the World Wide Web, the law enforcement community, postal and customs inspectors became aware of pedophiles' online commercial activities and websites (See Table 1). The resulting crackdown succeeded in destroying some communities, and in forcing others to move their servers outside the United States into countries that either had no laws restricting online child pornography, or in which Interpol had no jurisdiction. NAMBLA, for example, moved its operation to a server based in Denmark (http://www.nambla.org.de). The Rene Guyon Society and the Wonderland Society disappeared from the scene completely.

The next evolution in online child pornography was the move to the e-groups family of online communities, and to various Usenet newsgroups. Again, law enforcement pressure resulted in the pederasts' withdrawal from e-groups and the widespread "cleaning up" of newsgroups. As of this writing, the law enforcement community is only slowly becoming aware of pederasty occurring in the same file-sharing networks used popularly to trade copyrighted music and videos.

	Number of tips				
Technology	**1998**	**1999**	**2000**	**2001**	**2002**
Web sites	1,393	3,830	10,629	18,052	26,759
E-mail	117	165	120	1,128	6,245
Peer-to-peer	-	-	-	156	757
Usenet newsgroups & bulletin boards	531	987	731	990	993
Unknown	90	258	260	430	612
Chat rooms	155	256	176	125	234
Instant Messaging	27	47	50	80	53
File Transfer Protocol	25	26	58	64	23
Total	**2,338**	**5,569**	**12,024**	**21,025**	**35,676**

Source: Exploited Child Unit, National Center for Missing and Exploited Children.

Table 1. NCMEC CyberTipline Referrals to Law Enforcement Agencies, Fiscal Years 1998-2002. (Source GAO).

According to Doctor (Major) Nate Galbreath, USAF, and Doctor Al Cooper of the San Jose Marital and Sexuality Center, the Internet offers an accessible, affordable resource for the indulgence of paraphilic urges that provides a certain expectation of anonymity. "The 'triple-A engine' of accessibility, affordability and assumed anonymity allows for exploration of many sorts of paraphilic desires…."[60] The Internet, with its plethora of adult-oriented commercial and amateur websites, and the advertising spam they generate provides a way for people to "discover" and to seek to gratify their sexual compulsions. Moreover, treatment for paraphilic disorders often entails abstinence from going online at all, or at the very least strict (although not always successful) monitoring of their online activities.

Not all online pedophiles exist as members of communities. In fact, very few groups meet the definition of community as we have parsed it. Pedophilia is a solitary compulsion. A danger of the Internet is that by exposing pedophiles to others with the same compulsion, it can erode what behavioral inhibitions the fledgling paraphile may

[60] Galbreath, et al. (2002). p. 187

have. In some rare cases, pedophiles may operate in small, tight-knit cliques or teams. As Detective James McLaughlin of the Keene, New Hampshire Police Department puts it:

> Their organization typically centers on a few main players who often complain about the 'lurking' of the vast majority of those who join these groups. The motivation of different members is quickly apparent; some join to simply locate illegal materials (porn), others to meet children and others simply to talk about their arousal to children. The motivation determines how they interact.[61]

1. Purpose

Online groups or networks (if not communities) of pedophiles exist to indulge members' desires to view sexual depictions of children in erotic literature and images, to facilitate members' ability to contact children for the purpose of exploiting them sexually, and to provide support and advice. Often, communities exist to support pedophiles in their rationalized belief that their behavior causes no harm. BoyChat, part of FreeSpirits.org describes its purpose this way:

> BoyChat is a forum in which boylovers can explore issues related to their sexuality and provide mutual support and companionship - to learn to lead productive lives in ways that help young people rather than harm them (*sic*).[62]

Members of FreeSpirits try to differentiate their "community" oriented websites from their predecessors:

> The difference between NAMBLA and these new web sites, however, is that NAMBLA offered emotional support within a political context. The new web sites for the most part do not. There purpose is to provide emotional support, and build community regardless of a person's beliefs about the practice of man/boy love. (*Sic*)[63]

---

[61] Personal e-mail correspondence dated Friday, May 7, 2004.

[62] http://www.freespirits.org

[63] Public Posting on the Boy Chat online forum: http://www.ivan.net/bc/messages/95646.htm Posted by Dennis Bejin on May 03, 1998 at 18:05:21: Retrieved from http://www.prevent-abuse-now.com/pedoweb2.htm

On the FreeSpirits homepage, one can find several articles justifying pedophilia and, frighteningly, a link called ”Community Involvement” that gives the web addresses of several youth-oriented programs. The link includes a cynical disclaimer to the effect that the organization provides these links for those “sincerely wishing to involve themselves with their community in a positive way,” and in no way endorses using them as means to contact children.

McLaughlin places offenders into four general categories. McLaughlin studied over 200 offenders arrested by the Keene PD in a January 2000 Internet sting operation. McLaughlin’s summary, “Cyber Child-Sex Offender Typology” is online at http://www.ci.keene.nh.us/police/Typology.html.

Collectors: Collectors are persons who collect images and other erotica depicting children. According to McLaughlin, collectors frequent static sites on the Internet, such as newsgroups and web pages, where they believe their anonymity is assured. In some cases, collectors will leave the shelter of websites and newsgroups and become involved in much more dynamic interactions in chat rooms, where they are drawn into trading their material. Because pedophiles’ interests vary according to age, gender, ethnicity, setting and situation, they may require more and more interaction to satiate their specific needs. Many offenders learn the names of hundreds of files and image series, and immediately recognize materials they have already seen, even if it has been renamed. Given the vast amount of material available on the Internet, this ability demonstrates the time and effort collectors invest in their compulsion, averaging upwards of 12 hours per day.

In addition, collectors may use file-sharing software to trade in materials. “Real-time trading also involves some users setting up their computers as file transfer stations (FTP/Fservers). Users connect to these traders over the Internet and can see a directory of files that for which they can trade. The user uploads a child pornographic image file and receives credit to download the specific files he wants” (*sic*).

Travelers: The most dangerous type, travelers use trust building and manipulation to coerce their victims into face-to-face meetings. According to McLaughlin, “Over

half of these offenders represented their age falsely as being in their teens, and after some rapport revealed a more realistic, although still false, age. Over half of these offenders sent actual self-photographs; many were nudes. These offenders show many of the same traits as listed in Lanning's typology for "preferential/seduction" offenders."[64] Most of these offenders operate on the delusion that their victims are consenting partners, rather than coerced victims.

Travelers may journey thousands of miles, or pay for the victim to travel and even offer sanctuary for runaways. Sadly, approximately 1% of travelers are also sadists or murderers. In one case, police found photographs of several dead children in shallow graves on a suspect's computer.

Manufacturers: These are the collectors and/or travelers who have gone so far as to produce and distribute their own material. The Internet and wide availability of advanced multi-media capable computing has made this possible. Interestingly, the growth of the Internet and the spread of file-sharing technology has meant the near-destruction of commercialized child-pornography, in much the same way the music and film industry has felt threatened by Internet piracy and file-sharing. However, McLaughlin describes an operation run out of Russia that sold material on videotapes and CDs. Customers placed orders via e-mail, and routed their payments through international banks.

In conjunction with massively distributed file sharing networks, pederasts have the opportunity to remotely view and record lewd acts with children. Certain videoconferencing applications, such as CU-SeeMe[65], allow or require reflector servers. Reflec-

[64] FBI agent Kenneth Lanning distinguished two different types of sexual offenders—"preferential offenders" and "situational offenders." Preferential offenders offend due to a particular preference they have, such as for young boys. Situational offenders merely take advantage when an opportunity presents itself. Preferential offenders include various subcategories such as the "seduction type." Agent Lanning explained how seduction type offenders obtain control over victims by luring them with attention, affection, kindness, gifts and money. These offenders are typically unmarried, they have many boys visiting their home each day, they provide them with gifts, alcohol, etc., and they take the boys on trips and engage in massaging and other physical contact with them. These sex offenders are the most persistent, and have the greatest number of victims.

[65] CU-SeeMe is a videoconferencing program that combines audio, video and text-based chat capabilities. With CU-SeeMe, one can videoconference with another site located anywhere in the world. By using a reflector, one can see and communicate with a number of people from different sites at the same time. One can download the freeware version of CU-SeeMe for both Mac and Windows machines, or one can purchase a combination of camera and software from several online sites.

tors are simple relay programs that take several inputs and relay them to all the other participants. Any one of the participants can record anything he or she receives and then redistribute it. Per McLaughlin:

> Sex offenders have been caught numerous times sending computer cameras to under aged persons … so they could connect and view real-time sexual acts. There have also been criminal cases brought when an offender arranged with others to view himself engaging in real-time sex with a child victim on camera for others around the globe to view. [66]

Chatters: Not collectors of explicit, hard-core material, chatters skirt the law by viewing and possessing "naturist" depictions. Generally, chatters avoid transmitting or receiving material over the Internet, and often pose as "protectors" of children online, although their compulsion leads them to manipulate children into lewd or explicit conversations, ("cybersex" or "cybering") and often venture as far as soliciting or engaging in sexually oriented telephone conversations with their victims.

2. Restrictive Accessibility

Access is highly restricted. The ability to connect with servers, peers, or join newsgroups is often determined on the ability of a prospective member to secure a trusted contact with the necessary access who can vouch for the newbie's trustworthiness. Often, prospective members are required to upload new material in exchange for the privilege of downloading material from the pool. This solution to the free-rider problem is also a method of establishing trust. Members of these networks know that law enforcement officials are prohibited from possessing and transmitting illegal materials; however they have not, in the words of Detective McLaughlin "figured out we can take over the membership of someone who has been arrested."

3. Trust

Pedophile forums, such as FreeSpirits.org offer assurances of anonymity, p2p chat, and links to obtain anonymizing software and public key/secure socket layer en-

[66] McLaughlin. (2000).

cryption software. As discussed in the previous section, one can obtain access to their communities through what Sztompka terms “evocative trust”:

> There is a third type of *commitment* when we act on the belief that the other person will reciprocate with trust toward ourselves. In this case, we trust intentionally to evoke trust. *This is particularly characteristic for the close intimate relationships, among family members, friends and so forth, and is intended to make the bond even stronger*.[67]

Sztompka intended to describe the positive aspects of evocative trust, but evocative trust is most often used in situations where the *un*trustworthiness of the potential member or person seeking access is the *prima facie* assumption. People use trust, in this sense, to create strong rather than weak bonds. This fact provides a clue to such communities’ primary mode of connectedness.

4. Mode of Connectedness

The modes of connectedness of online pedophile “communities” vary with their members’ intent, with their level of paranoia, indeed, with their personalities. Most pedophiles seek only bridging ties – others who can connect them with the materials they crave. Some exhibit bonding behavior of varying strengths; mentoring relationships and sometimes friendships develop. A few groups, such as FreeSpirits, preserve the political agenda associated with older organizations like NAMBLA and offer support and rationalization for pedophilic behavior. These groups consist largely of a few (five to fifteen) core members who connect with each other and who attempt to present the image of a large, organized community.

Online pedophiles have taken increasingly to the use of peer-to-peer (p2p) networking in order to take advantage of the anonymity and safety they mistakenly believe they provide.

Peer-to-peer networks come in two basic varieties, centralized or decentralized (Figure 4). In the centralized model, a “broker” serves to mediate the transactions. Clients send requests to the broker, and the broker matches the request with the available

[67] Sztompka. (1999). p. 28. Emphasis mine.

files on members' hard-drives. If the broker finds a match, it provides the address of the provider, and the requestor connects directly with the provider's computer to download the file. The broker must maintain the addresses of all members, and can provide a comprehensive log of all the transactions it has brokered.

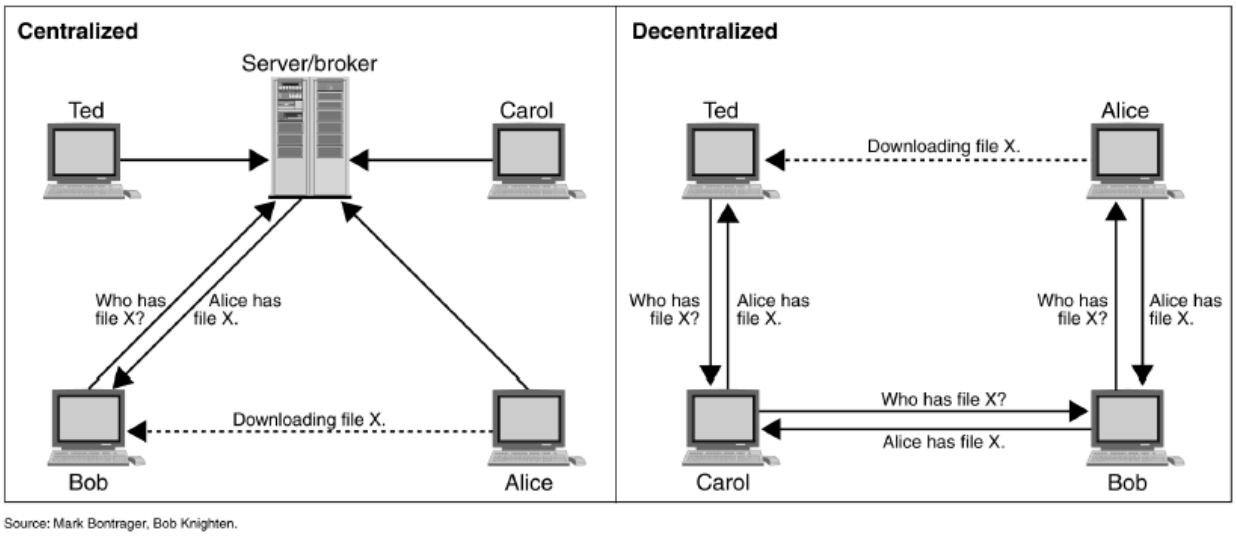


Figure 8. Peer-to Peer Network Models (Source: GAO)

In contrast, the decentralized model does away with the broker; intermediate peers handle the request and address response traffic. The decentralized network is a pure example of the small-world network problem. With no centralized database, the path-length from any given requestor to any given provider depends upon the overall *instantaneous topology* of the network. The topology is instantaneous because nodes (members) join and disengage continuously. A given request/response path length may range from two intermediate connections to several thousand, and the next request will be different yet again. The intermediaries may keep a log of the requests they have processed, but their view will be local, that is, limited to the machines with which they have direct connections. Once the requestor finds another who has the data they want, the two machines connect directly to facilitate the download. Attempts to attack these types of networks can only roll them up so far before the audit trail dries up. In such

cases, topological maps are perishable commodities, and have no predictive value. There is no guarantee that a given pedophile will connect along the same path beyond their local physical connection(s).

For these reasons, many online pedophiles are under the impression that the use of p2p networks guarantees their anonymity ("BoyChat is safe because it is anonymous. People don't have to show their faces if they don't want to."[68]) For example, one can find one of the most outspoken pedophile communities at http://www.free.spirits.org. FreeSpirits exists to attempt to justify "intergenerational sex," and to provide a social support network for pedophiles. FreeSpirits bills one of its services, LifeLines, as a p2p support group.

However, as the music industry demonstrated quite publicly, users of p2p networks are not anonymous and can be tracked. Moreover, as the GAO recently demonstrated, finding offensive material is rather easy (Figure 5).

It is likely, therefore, that while pedophiles will continue to use p2p technology, they will move increasingly to decentralized schemas, and employ cryptographic identification and authentication. Passwords are given to new members who demonstrate their trustworthiness, but titles, filenames and even the file types are likely to be encrypted and therefore invisible to the casual searcher.

[68] http://www.free.spirits.org.

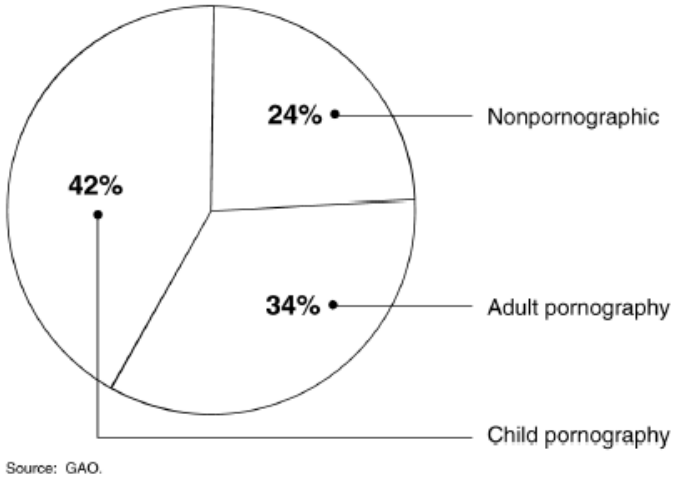


Figure 9. Classification of 1,286 Titles and Filenames of Images Identified through a Kazaa Search. (Source: GAO).

5. Transience

Decentralized p2p schemes are inherently transient. The network does not maintain connections over time, topology is dynamic, and peers generally do not employ logs and auditing. Nevertheless, a May 14 article appearing on CNN.com announced the arrests of dozens of persons using p2p networking to trade in child pornography. As law enforcement continues its crusade against child pornography, and pressure increases, online pedophiles may employ a sort of planned transience along with the move to the use of decentralized p2p schemes and encryption. AOL chat *rooms* are persistent, in that while the majority of their membership turns over in time, the forum tends to remain. *EverQuest*, as we have seen, is persistent because players tend to return repeatedly to play the game and to socialize with their online friends. Pedophile communities are likely to stage “events” or sessions in which they congregate online to trade material, but which will likely last only a short amount of time.

C. MEMBERS

It is important to discuss briefly the psychology of pedophilia and the influence of the Internet. Pedophilia belongs to a family of disorders known as Paraphilias, which includes a variety of sexually related compulsive disorders, such as transvestitism, voyeurism, exhibitionism, necrophilia, and paraphilic coercive disorder (rapists). According to one school of thought, one discovers one's sexual appetites, rather than learning them. Most people are able to suppress, redirect, ignore, or outgrow deviant urges; however, for paraphiles it is as impossible for them to stop their unacceptable behavior or suppress their urges as it is for someone to give up eating. Often, paraphiles experience severe distress and disruption in their lives due to the inordinate amount of time spent online that feeding their disorder requires, not to mention the terrible price many will pay should their behavior be exposed. At least one suspect in the Operation Candyman dragnet committed suicide in the wake of their arrest.

1. Network Capital

In order to feed their addiction using the Internet, pedophiles display all of the elements of network capital.

a. Access to Technology

By definition, online pedophiles have access to technology. As the Internet has increased in its ubiquity in the workplace, in homes, and in public places, access in most of the developed world has become easier and easier. Wealth still plays a role – to access the Internet from home, one must of course be able to purchase or rent the necessary equipment and services. A large proportion of paraphiles, however, access their materials from work. For example, in 1995, the former commander of an Air Force base in central Texas at which I was stationed was arrested and relieved of command for possessing child pornography, on both his home computer and his government-issue work computer. More recently, a respected physician at a major metropolitan hospital, with no criminal record and no history of molesting youngsters, was arrested for the possession of over 9,000 pornographic depictions of children on his office com-

puter. A father of two, who had never shown any sexual interest in his own children, the physician never considered the fact that the pictures he hoarded were the result of the criminal exploitation of children.[69]

b. Computer Literacy

Online pedophiles must marshal an above-average understanding of, and ability to use, computer mediated communications technologies. Web surfing, downloading, uploading, posting messages, installing and managing file-sharing software, using cryptographic software and protocols, and operating audio-visual equipment are just a few of the computer skills online pedophiles must master.

As noted earlier, many develop the ability to recognize files they have seen before based solely on the file properties (file size, contextual clues, file name variations, etc.) Table 2 shows a non-comprehensive list of technologies and their descriptions that can be and are often used to access child pornography.

[69] Galbreath, et al. (2002). p. 193-194.

Technology	Characteristics
World Wide Web	Web sites provide on-line access to text and multimedia materials identified and accessed through the uniform resource locator (URL).
Usenet	A distributed electronic bulletin system, Usenet offers over 80,000 newsgroups, with many newsgroups dedicated to sharing of digital images.
Peer-to-peer file-sharing programs	Internet applications operating over peer-to-peer networks enable direct communication between users. Used largely for sharing of digital music, images, and video, peer-to-peer applications include BearShare, Gnutella, LimeWire, and KaZaA. KaZaA is the most popular, with over 3 million KaZaA users sharing files at any time.
E-mail	E-mail allows the transmission of messages over a network or the Internet. Users can send E-mail to a single recipient or broadcast it to multiple users. E-mail supports the delivery of attached files, including image files.
Instant messaging	Instant messaging is not a dial-up system like the telephone; it requires that both parties be on line at the same time. AOL's Instant Messenger and Microsoft's MSN Messenger and Internet Relay Chat are the major instant messaging services. Users may exchange files, including image files.
Chat and Internet Relay Chat	Chat technologies allow computer conferencing using the keyboard over the Internet between two or more people.

Source: GAO.

Table 2. Technologies Commonly Used To Access Child Pornography. (Source: GAO)

c. Social Networking Ability

Pedophiles, of necessity, have had to develop social networking skills. The entire practice, shunned and justly vilified as it is, requires stealth and connections. The vilification of pedophiles has also posed formidable barriers to those seeking to understand their particular subculture. However, some insights are possible to find for legitimate researchers using the web. Often, websites established to disseminate the knowledge necessary to combat pedophilia offer excerpts from various sites, such as the "BoyLove Manifesto" which states the political objectives of pedophiles that participate in the FreeSpirits community. Certain hacking organizations exist for the very purpose of attacking pedophiles' networks[70]. Law enforcement officials pose as children and as pedophiles in order to penetrate these networks. However, none of these or-

[70] The most well known of these, Ethical Hackers Against Pedophilia (EHAP), conducted denial of service attacks against web-servers and message forums and did defacements of sites posting child-pornography. Additionally, EHAP often provided tips to law enforcement, identifying online pedophiles. However, their webpage, http://www.ehap.org no longer exists.

ganizations to this date has documented the social network structures or done the analysis necessary to understand their quarry's organization.

However, as Donna Hughes pointed out in the opening quote, the technology of the Internet makes it very easy for pedophiles to reach out to each other and find materials and moral support. In a sense, the Internet, as a manifestation of human social nets, has facilitated the networking behavior pedophiles have always used.

2. Trusting Behavior

As is evident by now, online pedophiles are not trusting individuals. Pedophiles keep their compulsions and behavior hidden, and many fail to seek appropriate help for their behavior until after they have been arrested. For this reason, online pedophiles tend not to act in groups. In McLaughlin's study, the vast majority of those arrested tended to live alone, and were socially isolated. This behavior is consistent other findings about sexual behavior online,[71] in that most people seeking sexual contact online do so because they feel they cannot meet their needs in real life, either because of their situation or the nature of their needs.

3. Cognitive Ability

According to McLaughlin,

> Pedophiles represent a range of intelligence, but on average test higher in intelligence than non-sex offenders. I have been a member of many of these communities and trust develops over time, which often leads to offenders' downfall by being arrested. Sex offenders are victims of cognitive distortions, which they use to justify their behavior. These permission-giving beliefs, rationalizations, take on more support in groups, creating intellectualization for their views on the 'benefits' of sex with children.[72]

[71] Cooper, et al. (2004), Young (1997), and Leiblum (1997).

[72] Personal e-mail correspondence dated Friday, May 7, 2004.

4. Education

As noted in Chapter III, wealth and education play an important role in who has access to the Internet, as well as in who is likely to be computer literate. In 1998, nearly a third of Internet users worldwide had a college education, and over 60 percent of college-educated persons in the United States used the Internet. This proportion has only increased in recent years. One would expect a rough correlation in the demographics of online paraphiles.

Table 3 shows a limited look at the educational backgrounds and behaviors of Internet outpatients receiving treatment at the National Institute for the Study, Prevention and Treatment of Sexual Trauma (NISPTST) in Baltimore, MD from 1998 through 2000. Of these patients, more than half had undergraduate or graduate degrees. Given the small sample size (*N*=36), and that fact that the information is self-reported, these results may or may not be representative of the population of online pedophiles. However, they are consistent with the demographics of Internet users in general, according to the UCLA study previously cited.

Sex	%	N
Male	97	38
Female[a]	3	1
Education	**%**	**N**
Less than high school	21	8
Diploma/G.E.D.	23	9
College degree (2 or 4 year)	28	11
Graduate degree (M.D., J.D., Ph.D.)	28	11
Paraphilic diagnosis	**%**	**N**
Paraphilia NOS	49	19
Pedophilia[b]	23	9
Voyeurism	8	3
Exhibitionism	3	1
None	18	7
Past psychiatric history	**%**	**N**
Mood (major depression)	21	8
Sexual disorder (paraphilia)	10	4
None	69	27
Criminal history	**%**	**N**
Prior history (as noted below)	36	4
Sexual contact w/minor	5	2
Indecent exposure	3	1
Solicitation	3	1
Sexual battery	3	1
Nonsexual criminal history	23	9
No known criminal history	64	25

Race	%	N
Caucasian	92	36
Hispanic	8	3
Employment	**%**	**N**
Attorney	8	3
Computer Specialist	10	4
Physician	10	4
Sales/retail	10	4
Service industry worker	10	4
Skilled laborer	21	8
Student	5	2
Unemployed/retired	8	3
Other (radio DJ, gov't, cook, etc.)	18	7
Reported internet behaviors[c]	**%**	**N**
Used sexually explicit Web sites	92	36
Used sexually explicit chatrooms	64	25
Identified during police "sting"	41	16
Identified due to public complaint	33	13
Identified by spouse or divorce proceedings	10	4
Reported use of computer at home	85	33
Reported use of computer at work	21	8
Comorbid disorder	**%**	**N**
Mood (major depression)	49	19
Substance abuse (alcohol)	13	5
None	38	15
	100%	
Nature of instant offense[c]	**%**	**N**
Attempted to meet a child for sex	33	13
Made no attempt to meet a child for sex	67	26
Sent pornography to a child[d]	28	11
Downloaded child pornography	54	21

Note: This data was gathered through a review of cases (N = 39) that entered the NISPTST between 1995 and Fall 2000 for sexual problems involving the Internet. Mean age of patients at time of evaluation was 41 (SD = 12.4), ranging from ages 17 to 70. Diagnostic data reflects those disorders identified at time of initial evaluation (Berlin & Galbreath, 2001).

[a] Our sole female patient was accused of Internet abuse by her spouse during divorce proceedings. She was evaluated and found to not be suffering from any sexual disorder.

[b] Includes those attracted to both prepubescent and adolescent children.

[c] Subjects may be included in one or more categories, or not included at all.

[d] Subjects transmitted child pornography to children, or to law enforcement agents whom they believed to be children.

Table 3. The Internet and Paraphilias: A Snapshot of 39 Internet Outpatients at NISPTST. (Source: Sex and the Internet: A Guidebook for Clinicians. p. 203)

D. CONCLUSION

We have seen how pedophiles exhibit all of the identified characteristics of networkers, although whether they truly exist online as "communities," even given a rather broad definition of community, remains at issue. Actual research into these communities and their structure is largely nonexistent, because the stigma (as well as the criminal penalties, since it's hard to study pedophiles without downloading child porn) attached to pedophilia and participation in such networks presents ethnographers with strong disincentives to enter these networks. Moreover, the users of p2p networks may soon move to rid themselves of the child porn problem in the same way that newsgroups did. Despite their general disdain for authority, p2p users do engage in normative behaviors and the use of informal social controls. According to Svensson and Bannister,

> In general, p2p participants are just as concerned — as most of us — when it comes to content issues such as (child) pornography or racism. They may even have an additional stake in fighting excesses, since illegal content may be the argument for authorities to take harsher measures. It might therefore be expected that users in p2p networks will take some responsibility for social control, albeit a limited degree of control. Indeed, this is what occurs. Some p2p users at least are prepared to address normative issues.[73]

Nevertheless, the use of p2p networks is interesting in itself. Given the high security requirements and evocative trust issues, p2p networks may provide the localizing infrastructure necessary to enhance flexibility while maintaining security in military networks. P2p networking can facilitate the ad-hoc information exchange architectures needed to support special operations forces in dynamic environments and in conducting unconventional warfare, and perhaps be more secure.

Certainly, the bad guys are making increased use of p2p networking, in addition to the use of e-mail, web pages, message boards and newsgroups. A similar broad-spectrum skill-set is therefore necessary for military and law enforcement agencies seeking to combat them.

[73] Svensson and Bannister. (June 2004).

I have structured the next case slightly differently than the preceding cases. I have done this to illustrate more fully the nature of the techno-social relationship, and how online behaviors reflect the *pre-existing* culture and sociology of the individual participants.

VII. CASE STUDY 4: ISLAMIST TERRORISM ON THE NET -- SOCIOLOGY AS TECHNOLOGY

A. INTRODUCTION

On November 18, 2002, *Computerworld* reported that

> Jihad groups around the world are very active on the Internet … the military wings of these various groups are using and studying the Internet for their own operations. … To date, al Qaeda's cybercapabilities have been the subject of much debate. Most Internet security professionals have doubted such groups' interest in cybertactics on the grounds that physical bombings and other forms of attack provide the fear and bloodshed that al Qaeda is looking for. However, in recent statements made by bin Laden, the terror leader has shown a clear desire to inflict catastrophic damage on the U.S. economy as a way to force the United States to withdraw its military forces from Afghanistan and to curtail its support for Israel.[74]

As the "Internet security professionals" cited above might attest, this sort of activity flies in the face of our traditional views of Islamist terrorists. According to most measures of who has access to computers and the practical understanding to use them effectively, one finds these characteristics primarily among those who are relatively affluent and who sport post-secondary educations. According to a report prepared under an interagency agreement by the Federal Research Division of the Library of Congress in September 1999, it is European and Japanese terrorists who "are more likely the products of affluence and higher education than of poverty," and not Islamic fundamentalist terrorist organizations.[75] Nevertheless, we see Islamist terrorists using CMCT to encrypt communications, marshal resources, recruit, organize, coordinate, transfer funds covertly, gather intelligence and plan attacks.[76] As recently as last year, al Qa'ida

74 Verton. (November 18 2002).

75 Hudson, et al. (September 1999).

76 According to Thomas Homer-Dixon, Professor of Political Science at the University of Toronto "new communications technologies—from satellite phones to the Internet—allow violent groups to marshal resources and coordinate activities around the planet. Transnational terrorist organizations can use the Internet to share information on weapons and recruiting tactics, arrange surreptitious fund transfers across borders, and plan attacks. …Information-processing technologies have also boosted the power of terrorists by allowing them to hide or encrypt their messages. …The Web also provides access to critical information. …Practically anything an extremist wants to know about kidnapping, bomb making, and assassination is now available online" (Jan-Feb 2002. "The Rise of Complex Terrorism." *Foreign Policy Magazine*. Retrieved 1 December 2003 from : http://www.foreignpolicy.com/issue_janfeb_2002/homer-dixon.html.

cells operating in the United States were using voice-over-Internet services to communicate with foreign-based cells, and computers captured in Afghanistan demonstrated that al Qa'ida was doing intelligence collection and transmitting encrypted messages over the Internet. Timothy L Thomas, writing for *Parameters*, states "the Internet provides terrorists with anonymity, command and control resources, and a host of other measures to coordinate and integrate attack options."[77]

In previous chapters, I have described communities and members according to the typologies laid out in Chapter III. In this case study, I want to emphasize the concept of network capital exclusively, to illustrate more fully the relationship between sociology and technology discussed in Chapter I.

B. COMMUNITY DESCRIPTION

As stated in the introduction, Al Qa'ida uses high-tech methods including E-mail, Internet Relay Chat (IRC), Web-publishing and steganography in conjunction with low or no-tech methods like messengers, informal money transfers, and smuggling to achieve its logistic, intelligence, and operational communications objectives. Al Qa'ida is capable of recruiting members that can blend into their respective target societies and need little communication with the core organization.

Joel Garreau[78] of the Washington Post makes a number of interesting points about how to attack a network like Al Qa'ida. Garreau supports John Arquilla's idea that "it takes a network to fight a network" and considers intelligence crucial to analyzing a network's *weak* ties. Garreau and Arquilla believe that targeting trust or loyalty can destabilize a network. However, a network like Al Qa'ida may prove a very difficult target. Al Qa'ida, reflecting the socio-cultural context in which its members are embedded, is a largely decentralized, "small-world" network, consisting almost exclusively of *strong* ties.

Al Qa'ida's distributed, ad-hoc topology lends itself to an efficient distribution of labor among planning and intelligence-gathering cells and operational cells. Cells can

77 Thomas. (Spring, 2003). p.116.

78 Garreau. (September 17, 2001). p. C01.

self-organize or dissolve in response to perceived threats and vulnerabilities while maintaining secrecy because of their strong ties and localized perspective. The smooth functioning of the network over long periods is an outcome of trust (some negative, some positive) between its members, strengthened by kinship or common experience, ideology and a common purpose. The network avoids defections through the application of social pressure and mutual social control.

This particular point is important. Al Qa'ida's topology is not all hub-and-spoke, circular, nor even "all channel," as some have asserted. Because Al Qa'ida is a highly networked umbrella organization, its topology is determined *locally*; reflecting the social structures, missions, and threat environments of each cell, and therefore of each individual. Al Qa'ida replicates its peculiar ad-hoc topology in cyberspace, although without a dedicated or formal routing architecture.

Carley, Lee and Krackhardt's analysis[79] reaffirms what we know about networks like Al Qa'ida – it is a Hydra: cut off the head and two or three grow back in its place. This reflects the socio-cultural context of its membership. Leadership is not an indicator of one's ability to influence the social network as a whole. Leadership position in network societies is a product of strategically formed *weak* ties in the influence net – the emergent result of flows of information from others who are well-embedded in the knowledge or information networks, and who have benefited materially from the actions of the would-be leader.

> There is a dilemma in tribal societies: the very tool which enables tribal leaders to establish powerful political entities, the charter of segmentary solidarity, is also instrumental for segmentary division. Once a charismatic leader who masters the instrument of segmentary alliance loses influence or dies, the divisive character of the segmentary tribal system will gain the upper hand. Tribal systems do not usually develop institutionalized political power that could tolerate fluctuations in the abilities of individual rulers. [80]

Thus, even in the predominantly strong-tie social network of Al-Qa'ida, the one who can marshal the power of weak ties is the leader. This is Usama Bin Ladin's par-

[79] Carley, et al. (2002). pp. 79-92.

[80] Glatzer. (2002). p. 271.

ticular genius: he is at once a Connector and a Salesman. However, the strong-tie nature of the network makes it resilient against the loss of any one leader.

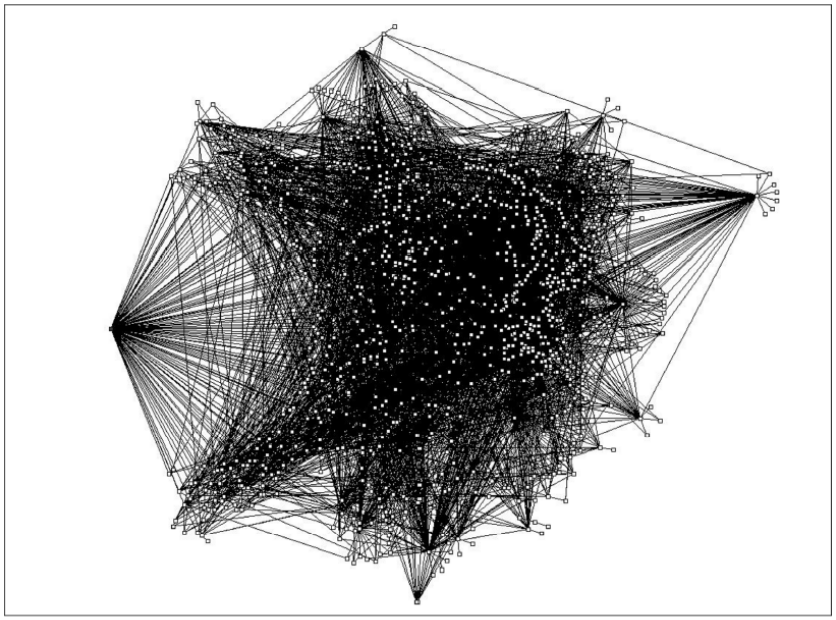
Decentralized p2p networks such as Gnutella[81], Kazaa[82], or Freenet[83] (see Figure 9), whose basic functioning we discussed in the previous chapter, are particularly well suited to support strong-tie social networks like Al Qa'ida. Each peer is aware only of the peers with which it has direct connections – a purely localized perspective; although in p2p networks proper, new connections are readily established and nodes keep a list of their connections in a cache. No single peer or broker maintains directory information relating content to specific peers (IP addresses, etc) for the entire network. The absence of a meta-database, either central or distributed, greatly simplifies operations, while simultaneously hindering hostile intelligence gathering. Anonymity and encryption technologies further complicate the process of mapping such networks.

These features make p2p particularly effective for groups who wish to conceal their communications, as evidenced by the experience of online pedophiles. Interestingly, Al Qa'ida's use of p2p networks is small in comparison to its use of more mainstream CMCT applications, such as chat rooms, e-groups, web publishing, e-mail, and encryption. However, the pedophiles moved to the use of p2p only after the efforts of various nations' law enforcement agencies and private activists thwarted their use of more conventional methods by directly taking down web sites, and arresting members. Should the GWOT have a similar effect, it is possible that al Qa'ida will increasingly adopt the use of p2p. It could also be that the pedophiles as a whole are more educated and technologically savvy than al Qa'ida as a whole – al Qa'ida leaders clearly are, but very few of the foot soldiers. Pedophiles are mostly middle class, educated males as we have seen. Using p2p requires more sophistication than the web because it requires special software.

81 Kurose and Ross. (2003). pp. 165-172

82 Koontz. (September 9, 2003).

83 Sandberg and Wiley. (Spring 2002). p.41.



Source: Mihajlo A. Jovanovic, Fred S. Annexstein, and Kenneth A. Berman, Laboratory of Networks and Applied Graph Theory, University of Cincinnati.

Figure 10. Instantaneous Topology of a Decentralized Peer-to-Peer Network (Gnutella) (Source: GAO)

For the moment, however, Al Qa'ida continues to make broad use of conventional CMCTs in its operations, as Dorothy Denning enumerates in her May 2004 article "information operations and Terrorism."[84] Recently, the Al Qa'ida-affiliated publication Al-Sharq al-Awsat announced the creation of an "Internet University," claiming that hundreds of Muslims are joining, and that some specialists and leaders have already graduated. Michael Knapp, an asymmetric warfare analyst at the National Ground Intelligence Center (NGIC), describes the "university" as a follow-on to the Mujahideen Services Bureau (MAK) and a possible virtual replacement for lost ops bases and training camps in Afghanistan that is designed to teach "all jihad sciences and their rules and types."[85] The university offers specialties in: "electronic jihad," "media jihad," "jihad with self and money," "technology of explosive devices" and "booby trapped cars and vehicles." Clearly, the Internet University would also function as a vehicle for recruiting and

[84] Denning. (May 17, 2004).

[85] Knapp. (2003).

ideological training as well as technical instruction. Its faculty supposedly consists of mujahideen leaders, headed by UBL ("Dean of the Podium of the University").

Despite such ominous developments, there is little reason to expect successful "cyberattacks," per se, anytime soon. RAND researchers Grey Burkhart and Susan Older tabulate the cyber-capability of Islamist or opposition groups in their 2003 report The Information Revolution in the Middle East and North Africa. Their results indicate that the threat posed by Usama bin Ladin is perhaps less than we fear, while externally based political opposition groups such as the CDLR [*Lajnat al-Difa' 'An al-Huquq al-Shar'iyya* or Committee for the Defense of Legitimate (Islamic) Rights] possess far greater capabilities (Table 4).

Moreover, as two publications of the Center for the Study of Terrorism and Irregular Warfare (CSTIW) indicate, there is a fundamental difference between the psychosocial behavior of virtuoso hackers and the psychosocial behavior of Islamist militants.[86]

Nevertheless, one must ask why and how are Islamist terror groups, despite their reactionary ideology, so adept at using the Internet to organize, finance, and equip themselves? The obvious answer is that educational attainment explains Islamist terrorists' facility with computer-mediated communication technologies. Indeed, most leading members of Al Qa'ida, far from being poor, uneducated cretins, are in fact highly educated intelligent men; who all happen to share an extreme sense of (misdirected) outrage against Western culture in general, and the policies of the United States specifically. As we have seen, however, access to technology and computer literacy do not fully account for network capital. A familiarity with social networking is also essential. There is good reason to believe that it is from their own cultures that Islamist terrorists draw the final component of network capital.

[86] CSTIW. (2000), and Nelson, et al. (1999).

Country	E-Government Rating[a]	Opposition "Loyal" or Otherwise	E-Opposition Rating[b]
Algeria	None	AIS	None
		FIS	None
		GIA	None
Bahrain	Moderate	Misc. Islamists	None
Egypt	Moderate	Islamic group	None
		Misc. opposition	Low
Iran	Low	"Hardliners"	Low
Iraq	None	Everyone	None[c]
Israel	High	Hamas	Low
		Hizbollah	Low
		Misc. Palestinians/groups	None
Jordan	Low	None significant	na
Kuwait	Moderate	Misc. politicos	Low
Lebanon	Low	Opposition parties	Low
		Syrian intelligence	Very Low
Libya	Very Low	Everyone	None
Morocco	Low	West Saharans	None
Oman	Low	Misc. Islamists	None
Qatar	High	None significant	na
Saudi Arabia	Moderate	CDLR (external)	High
		Misc. Islamists	Low
		Osama bin Laden	Low
Syria	Very Low	Muslim brotherhood	None
		Non-Alawite activists	Low
Tunisia	Low	Opposition parties	Low
UAE	High	None significant	na
Yemen	Very Low	Misc. tribes	None
		Unreconstructed Communists	None

[a]A factor of the degree of automation and networking internal to the government and externally with the populace.

[b]A factor of the degree of automation and networking internally and on the Internet.

[c]Various opposition groups in exile have a limited external Internet presence that is transparent to residents of Iraq. There is limited Internet connectivity between some Kurdish-controlled areas and the outside world, mostly for coordination with and fund-raising by supporters in exile.

Table 4. Electronic Correlation of Forces. (Source: Burkhart and Older)

C. NETWORK CAPITAL: SOCIAL STRUCTURE AS TECHNOLOGY

Society is an emergent phenomenon, determined by the complex behaviors of its constituent individuals. However, society also exerts a strongly deterministic influence on individual action through normative processes in a dynamic Ouroborian cycle.[87] In highly networked societies, social connectedness *is* the technology used to ensure co-

[87] Sztompka describes this dynamic relationship well (1999. pp 3-4); however, I take issue with his assertion that individual action is the ultimate determinant of cultural emergence. The ultimate determinant in my view is the process itself, for without the dynamic interplay between individual agency and collective norms, societies would not evolve, and cultural stasis would ensue.

operation and coordination, and to provide the basis of trust necessary for the smooth functioning of the society. The use of CMCTs, as a physical manifestation of this mode of connectedness, may be intuitive to members of such societies, because they and their members are steeped in social networking.

The problem becomes the reverse of that encountered in our study of AOL chats; where AOL members had access to technology and computer literacy but lacked social networking ability, members of highly networked societies have the fluency, but may lack technological access and literacy.

1. Access to Technology

The origins of Islam, and therefore the heart of cyber-savvy Islamist dissident groups such as MIRA (Movement for Islamic Reform in Saudi Arabia) and the ARC (the Advice and Reform Committee, from which Al Qa'ida sprang), lie in the Middle East. Therefore, it is logical to expect that the Middle East with its oil wealth and free public education would enable access to CMCT. However, according to a September 2002 study by NUA, of the approximately 605.6 million people world-wide with access to the Internet, only about 5.12 million were located in the Middle East, comprising a range from about 0.3 percent of the population in Yemen to about 36.8 percent of the population in Bahrain.[88] Interestingly, Saudi Arabia was one of the lowest, with only 2.5 percent of its population having Internet access. According to the World Bank, in 2001 there were approximately 32 computers per 1,000 people in the Middle East and North Africa.[89]

Indeed, as indicated in Table 5 below[90], wealth plays a role in CMCT development; however, the Middle East and North Africa remain below world averages – and well below American standards – for Internet access and computer literacy, as we shall see. As the table also shows, Internet access is expanding rapidly in the region. This

[88] http://www.nua.com/surveys/how_many_online/index.html

[89] http://devdata.worldbank.org/data-query/

[90] Burkhart and Older. (2003). p. 48.

development brings with it increasing insecurity for the region's authoritarian regimes[91], and increased opportunities for Islamist opposition groups to transmit their messages. The challenges that will attend as the information revolution spreads across the Middle East will be manifold, and the outcome remains uncertain. What is clear is that the current crop of Islamist terrorists and dissident groups who arose in the last 20 years must have acquired their Internet know-how outside the region, by studying, living, and/or working abroad.

Disposition Type	Country	Wealth	Internet Development
Driven	Bahrain	High	Rapid, extensive
	Egypt	Moderate	Moderate
	Israel	High	Rapid, extensive
	Jordan	Moderate	Slow
	Kuwait	Very high	Rapid
	Lebanon	Growing	Rapid
	Morocco	Moderate	Moderate
	Oman	Moderate	Slow
	Qatar	High	Rapid
	Yemen	Low	Very Slow
Fearful	Algeria	Low	Halted
	Iraq	Low	None
	Libya	Low-moderate	Recent, slow
	Syria	Moderate	Recent, slow
"Best of Both"	Iran	Moderate	Very slow
	Saudi Arabia	Very high	Recent, moderate
	Tunisia	Moderate	Moderate
	UAE	Very high	Rapid

Table 5. Wealth and Disposition Versus Development Among Middle Eastern States (Source: Burkhart and Older)

2. Technological or Computer Literacy

Generally, the factors characterizing access to technology in a given nation also appear as measures of its people's computer literacy. Tables 6 and 7, compiled by

[91] Although Kalathil and Boas (2003. Open Networks, Closed Regimes.) show that expectations of the Internet threatening the security of authoritarian regimes are not well founded, certain regimes, most notably the Saudi Government, have spent a great deal of time, money, and diplomatic effort attempting to shut down the efforts of internet-using dissident groups operating in foreign countries. [See Fandy. (February 2001). Entire.]

Burkhart and Older,[92] are typical of the types of data available. What the RAND data and data from the online World Bank Knowledge Assessment Matrix[93] indicate is that computer literacy in the Middle East and North Africa, while far behind American or European standards, is generally increasing in pace with the penetration of CMCT – at least in those countries where the state supports such development. Again, the Islamist terrorists arising over the last twenty years must have achieved at least a tertiary level of education and/or traveled, worked, or lived outside the region.

MENA Country	Telephones per 100 Inhabitants	Personal Computers (PCs) per 100 Inhabitants	Internet Users per 10,000 Inhabitants
Algeria	6.36	0.71	19.27
Bahrain	67.15	14.18	1,988.65
Egypt	14.63	1.55	92.95
Iran	18.70	6.97	62.29
Iraq	na	na	na
Israel	128.46	24.59	2,304.86
Jordan	27.12	3.28	409.11
Kuwait	48.79	13.19	1,014.71
Lebanon	40.74	5.62	858.00
Libya	11.83	na	35.84
Morocco	19.60	1.31	131.45
Oman	21.34	3.24	457.49
Palestine	16.82	na	181.21
Qatar	56.76	16.39	655.74
Saudi Arabia	25.81	6.27	134.40
Syria	12.09	1.63	36.12
Tunisia	14.90	2.37	412.37
United Arab Emirates	111.66	15.83	3,392.39
Yemen	3.01	0.19	8.89
United States	110.87	62.25	4,995.10
World Averages	32.77	8.42	823.24

NOTE: na = not available.

Table 6. Indicators of Societal CMCT Penetration in Middle Eastern States, 2001 (Source: Burkhart and Older)

[92] Burkhart and Older. (2003). pp. 4, 8.

[93] http://devdata.worldbank.org/data-query/

Technology Dimension	Business/ Financial Dimension	Political/ Governmental Dimension	Social/ Cultural Dimension
Degree and nature of IT penetration into society	Amount of information work and number of information workers	Presence (and number) of new political actors (e.g., NGOs)	Degree of societal tension created because of IR developments
Distribution of IT activity across technology, artifact, and service spectrum	Amount and nature of e-commerce Presence (and number) of IT business clusters	Degree to which the role and manner of governance has changed	
Amount of "creative destruction"			
Movement of talented, IT-trained people (into and out of country)			

Table 7. Resultant Factors Characterizing a Nation's Internet Readiness Posture (Source: Burkhart and Older)

3. Social Networking Ability

a. Communal Societies

Various anthropologists and authors describe the traditional societies of southwest and central Asia as "small world networks,"[94] in which every member is related by blood, marriage or obligation to every other member. This particular feature,

[94] Kleinberg. (1999). "A social network exhibits the small-world phenomenon if, roughly speaking, any two individuals in the network are likely to be connected through a short sequence of intermediate acquaintances. This has long been the subject of anecdotal observation and folklore; often we meet a stranger and discover that we have an acquaintance in common. It has since grown into a significant area of study in the social sciences, in large part through a series of striking experiments conducted by Stanley Milgram and his co-workers in the 1960's (Milgram 1967, Corte and Milgram, 1978). Recent work has suggested that the phenomenon is pervasive in networks arising in nature and technology, and a fundamental ingredient in the structural evolution of the World Wide Web (Watts and Strogatz 1998). Milgram's basic small-world experiment remains one of the most compelling ways to think about the problem. The goal of the experiment was to find short chains of acquaintances linking pairs of people in the United States who did not know one another. …Over many trials, the average number of intermediate steps in a successful chain was found to lie between five and six, a quantity that has since entered popular culture as the "six degrees of separation" principle."

along with segmentary opposition and segmentary solidarity, is the apparent source of (variously):

- The decades-long civil war in Afghanistan,
- The failure of States like Iran, Iraq, Saudi Arabia, and Afghanistan to develop into western-style bureaucratic democracies,
- The existence of repressive regimes in such States, and the utility of organizing the post-Taliban government in Afghanistan along traditional tribal lines.

Islam, and its modern-day fundamentalist interpretations, developed and spread in a social context characterized by tribal networks; moreover, its spread was enhanced by and dependent upon such networks: Despite the explosive expansion of Islam in the twelfth through fourteenth centuries, it succeeded and remains strong among peoples whose societies were originally tribal. Tribalism, however, is not really the right word to describe the social dynamic at work.

Defining tribalism is difficult. It has a variety of meanings depending on the social context, and can describe genealogies as well as particular forms of political organization. Tribalism has come to connote a primitive form of social organization; however, it is not at all clear that it is indeed primitive. Tribalism is neither a vestige of the past, nor a stage of development between "bands" and "states." It is not "primitive" as opposed to modern states. Tribes are not mere fringe groups on civilization's periphery. They are not invented ethnographic fictions or affectations. Tribes are not all composed of pastoral nomads: there exist settled, village, and urban tribesmen. They are not the ethnographer's ideal tribe (small, primitive, isolated, simple and self-sufficient); many are very large and complex. They are inseparable from their wider context, culturally and economically. Tribes are flexible, ever-changing groups that grow and decline, depending on many variables. What is common to tribalism is that it exists among – and partially defines – peoples that value communal life, with an attendant communal identity. Tribalism implies a network of bonding (strong) ties. Per Kali:

> Strong ties connect people within a network. Weak ties connect across networks. In subsequent work, Granovetter demonstrated that these different types of social capital are useful for different purposes. Weak links are better for collecting information (increasing connectivity) while strong links are important for fostering cooperation (overcoming the prisoners' di-

> lemma) and coordination. Two agents are connected through a weak link if they have few common neighbors and they are connected through a strong link if their neighbors overlap to a large extent. The presence of strong ties does not necessarily imply the presence of weak ties. Societies with high levels of embeddedness are likely to have strong ties[95]

Hereafter, when the word tribe or any of its derivations is used, it is with the tacit understanding that it refers to a highly networked communal society, consisting primarily of strong ties. The same need to ensure cooperation and coordination that drives the formation of clandestine communities as described in previous chapters is at work in tribal societies. It is the basis of the system of segmentary solidarity and segmentary opposition that characterize tribal societies. This is not to say that tribal societies necessarily resemble clandestine communities in character or purpose, but rather, they draw their structures from a similar need for security. It is one of this study's hypotheses that such communal societies and the communal identities they create contribute to network capital through cultural embeddedness of individual action.[96]

Despite ongoing urbanization and the modernization efforts of modern Arab states, tribal communities, with their associated forms of nepotism, patrimonialism, social status, and distribution of economic opportunities and resources continue to be strong factors, extending from state policies for regime maintenance down to the individual.[97] A lack of wealth also encourages strong ties, and therefore communalism.[98]

F. Gregory Gause III, of the University of Vermont, quite correctly points out that Islam and tribalism, as they exist today in modern Arab *rentier* states, are quite different from the traditional concepts most Americans associate with the Middle East. The Saudi regime specifically has based its legitimacy on self-constructed concepts of

---

[95] Kali. (January 2003). p.5.

[96] Sztompka. (1999). p. 2.

[97] Dr. Glenn Robinson confirmed the pervasive nature of tribal influence in modern Saudi society in response to the author's questions during a lecture in December 2003; part of a seminar in Low Intensity Conflict in the Middle East, conducted at the Naval Postgraduate School, Monterey, California.

[98] Ithiel Pool observes that "'the utility of weak links is a function of the security of the individual, and therefore of his wealth. A highly insecure individual, for example a peasant who might starve if his crop fails, is under strong pressure to become dependent upon one or a few strongly protective individuals. A person with resources on which he can fall back can resist becoming dependent on any given other individual and can explore more freely alternative options'." Granovetter (1983), pp. 201-233.

tribalism and Islam. Regimes design such policies to subordinate the power of the tribes and the clergy themselves into the service of the state through the distribution of oil rents in exchange for loyalty (patrimony). As a result,

> Citizens of these states are permitted to organize socially and participate politically through these sanctioned institutions. The governments supply money to support tribal and religious institutions, and allow them the space to operate publicly. That public space is largely denied to other types of social and political organizations like political parties or, with some limited exceptions, a free press.
>
> The unintended consequence of this policy has been to encourage political opposition, when it arises, to organize on *tribal and religious bases, both ideologically and institutionally*.[99]

b. Islamic Identity

Islam itself contributes to communal identity. For example, S'ad al-Faqih, of MIRA (Movement for Islamic Reform in Saudi Arabia) criticized the West for its lack of communal life, its "'indulgence in self-centered themes whereby individuals seek to maximize their own enjoyment at the expense of the larger society.'"[100]

Muslims have traditionally defined themselves as belonging to a global identity, or *Ummah*, a network that transcends national boundaries.[101] Another large body of evidence indicates a network of ties between radical Islamic groups and Islamic welfare organizations around the world. There is a presumption that being a Muslim, a member of the *Ummah*, automatically commits one to the cause of Islam, despite the wide variety of ethnic and national groups. Many of the charitable Islamic groups feel bound to support any group identifying itself with Islam, and may not even realize that they are in fact supporting terrorism. [102]

---

[99] Gause, F. (1994).

[100] Fandy. (February 2001). p. 156

[101] Lubeck. (2002). p. 76

[102] Milward and Raab. (October 2002). p.11.

c. Other Social Influences

Homophily is a term from biology, denoting similarity through common ancestry. In its sociological context, homophily generally means the tendency to interact with others who are similar to us. Homophily can arise from any number of traits shared in common, and tends to increase among individuals who share little with those around them. Shared experience and perspectives contribute to homophily. Tribal (read as communal) societies, such as the Arab and Bedouin societies native to the Middle East, tend to be strongly homophilous. Certainly, the 9/11 hijackers shared strong ties based on Islamic values, family connections and shared experience. As Krebs points out,

> The (9/11) hijackers' network had a hidden strength – massive redundancy through trusted prior contacts. The ties forged in school, through kinship, and training/fighting in Afghanistan made this network very resilient. These ties were solidly in place as the hijackers made their way to America. While in America, these strong ties were rarely active – used only for planning and coordination. In effect, these underlying strong ties were mostly invisible during their stay in America. It was only after the tragic event, that intelligence from Germany and other countries revealed this dense under-layer of this violent network.[103]

The homophily displayed by the al Qa'ida network can also be explained as originating in the individual sense of alienation experienced by each member, as Milward and Raab point out in their treatment of the al Qa'ida network. [104] In addition, as Granovetter points out, "low-status individuals are so numerous that it is easier for them to pick and choose as friends others similar to themselves."[105] These arguments tend to ignore cultural embeddedness of individual action in favor of social pressures in the immediate environment. Nonetheless, the importance of socialization in cognitive development and lifelong behavioral patterns cannot be understated, and clearly plays a role alongside the causes identified by Granovetter, Milward and Raab. Put simply, individuals socialized in communal societies will seek community in any subsequently encountered social environment.

---

[103] Krebs. (2002).

[104] "The key to understanding the attraction seems to be the sense of identity Al Qaeda gives these men. Especially young Muslim men in Europe who are alienated from their home countries but at the same time not at all integrated in their host countries." Milward and Raab. (2002). p.10. Emphasis mine.

[105] Granovetter, M. (1983). p. 210.

D. CONCLUSION

There is clear evidence to support a strong correlation between computer-mediated network aptitude and acculturation. There is also evidence to indicate that this ability may be self limiting, because of a general lack of trust in CMCT among Islamists, exacerbated by the success of counter terror operatives in ferreting out network data. Zanini and Edwards point out a number of operations in which the FBI and CIA were able to unravel subnets based on information extracted from captured computers, wire-taps, and captured suspects. As they put it,

> the organizational benefits associated with greater IT must be traded off against the needs for direct human contact and improved security. This makes it likely that terrorist groups will adopt designs that fall short of fully connected, all channel networks.[106]

Although p2p technology would be a logical and appropriate choice for al-Qa'ida, it is unlikely that they will adopt it unless pushed into it, in much the same way that pedophiles were forced to adopt its use. Currently, al-Qa'ida continues to use the Web and the Internet extensively, in part because of its efficiency, but also because of their perception that it offers greater security.

Further research, including controlled case studies, is required to confirm or deny this hypothesis. Exploring this question is important, because the answer may enhance our capability to predict and defend against the methods by which the Attas and Yousefs of tomorrow may use computer-mediated communications to threaten their targets.

The localized nature of al-Qa'ida's strong-tie social organization has important implications for the ways in which our military must confront them. Special operations forces, because of their regional divisions, are most capable of collecting and using local intelligence against local sub-nets. A problem of centralized command and control is that it is inefficient when faced with the information intensive nature of combating networked organizations. Centralized command and control tends to over-use cognitive shortcuts, applying generalized templates against diverse threats.

[106] Arquilla and Ronfeldt. (2001). p.40

VIII. CONCLUSIONS

A. INTRODUCTION

Who networks? The answer to this question is as much dependent upon the attributes of the networks to which people belong as it is upon the attributes of the participants themselves. This chapter brings together the ideas and information presented in the previous seven chapters to answer this question. Additionally, this chapter provides recommendations based on the information obtained about how the government and the military can make better use of CMCTs, and recruit personnel suited to networked operations.

B. FINDINGS

For the last decade, information operations and information warfare have worn the shiny-newness of our developing CMCTs. However, the real value of CMCTs has been to make us think seriously about the nature of networks – and netwar. An understanding of the nature of networks should make it clear that networks are most effective when allowed to react locally to local conditions. The use of cognitive shortcuts (mostly over-generalizations) is woefully inadequate when dealing with the multiform threats the United States faces in the twenty first century.

Given our characterization of online communities, some important ideas stand out. *Purpose* is by far the most important aspect governing community formation and persistence. Shared interests and trusting relationships are not enough to create and maintain a community. Purposeful communities survive best when the *goals of the community and the goals of individual members are congruent*, because this evokes a *personal commitment* from members. This holds true even when there is significant existential pressure applied to them. In such cases, they are able to employ tactical transience. Moreover, *distributed authority* and *informal lateral communications channels* permit networks to *respond locally to local conditions*, enhancing community persistence, especially in the case of already existing communities and organizations.

For individual members of networks, common purpose is key to creating a common identity. Common identity depends not only on shared purpose, but also on the

proximity of others in time, space, and context, which is to a large degree dependent upon *regular participation and interaction*. Because cyberspace may be more properly thought of as an interaction space, rather than an information space, *informal lateral communications* can enhance locality by facilitating interaction. *Social enforcement mechanisms* can be effective even in the absence of physical enforcement when community goals and personal goals align. Acts of *evocative trust*, as Sztompka points out, are necessary for the formation of strong ties; but shared purpose and common identity is required also to bind people in a network. Those who succeed in network organizations must possess social capital, and its online derivative, *network capital*.

What should also be clear from the case studies is that there are better uses of CMCT than those currently used by our military. We have neglected the social aspects of the technology in favor of a purely mechanistic, utilitarian perspective. Serious changes are required in the ways we organize, train, and fight if we wish to maximize the advantages CMCT confers. This does not imply that human nature or social behavior has changed because of CMCT; instead, it requires a re-evaluation of the role CMCT can play.

C. RECOMMENDATIONS

As this thesis has attempted to demonstrate, the threats we face and the civilian organizations we are bound to work with are adopting modes of connectivity (technical, social, and organizational) that we are ill suited to follow. Our leadership and command structure is dangerously out of step with the threat environment. Our intelligence agencies continue to share information based on inefficient models of connectivity. Originating agencies, which through the web page-based approach implemented on IntelLink have created cyberspace fiefdoms for themselves, stovepipe and jealously guard information and access. Information operators –*netwarriors* – must be capable of filtering and processing relatively large amounts of data, through multiple interface methods, and among many different connections, *and do so more laterally than vertically*. Within the scope of this study, four distinct areas for application exist: leadership and organiza-

tional culture, intelligence information communications architecture, special operations/unconventional warfare, and identifying and recruiting netwarriors.

1. Leadership and Organizational Culture

The current, highly centralized way in which our military's organization and communications technologies are oriented is insufficient to cope with the global, networked nature of current threats. Moreover, the principle of unity of command has been taken to its absolute extreme in the name of command responsibility. Because commanders are held accountable for the actions of commanders and personnel at all levels under them, there is great personal and hence organizational pressure to pass information to the top, where it is allowed to trickle down – along with sometimes-absurd orders. For example, following the 9/11 attacks, DoD placed *all* U.S. military bases at the highest force protection level – regardless of the actual threat posed to individual bases. Moreover, because the highest force protection level, Delta, was never intended to be implemented for prolonged periods, *local* commanders implemented *local* "modifications" to permit continued operations, albeit at a diminished level of efficiency. Some would say that that is exactly the way the system should work, and that the ability to make modifications is an indication of the system's flexibility. How much more efficient could the domestic response to 9/11 have been if commanders and their force protection advisors were given the authority to determine the appropriate force protection levels for themselves?

With the tremendous increase in available information, military commanders must be aware of their limited capacity to absorb, comprehend, and act correctly upon the information presented to them. Delegating authority requires commanders at the highest levels to trust their subordinates down the chain of command. Unfortunately, the quantity of information available to commanders and the speed with which it can be delivered gives them a false sense of cognitive mastery of remote and very complex situations and environments. There is also pressure that arises from the expectation of absolute responsibility and accountability placed upon commanders. When subordinates make mistakes (and they are bound to make mistakes) or act illegally, command-

ers must accept full accountability. The illusion of mastery, coupled with a *distrust* of subordinates has meant that DoD has spent millions of military dollars increasing the flow of information back from the front, instead of laterally across it.

As Jansen asserts,

> Environmental complexity does have the potential to generate information overload that degrades the performance of decisionmakers. …As the information load increases, decisionmakers increase the amount of information processed, but only up to a point. As information continues to increase, the information being processed does not simply reach a plateau; instead, there is degradation in the amount of information processed. …Centralization to a single decision-maker makes sense only to the extent that he or she has the requisite capacity, and requisite variety of information processing skills to match the environment. The same law of requisite variety holds for groups. Thus centralization in complex environments typically generates on organizational misfit[107]

The traditional model of hierarchical military leadership is still in force. CMCTs are inherently ambivalent, and can be used to support vertical flows of information as well as lateral flows. However, current organizational theory indicates that continued reliance on traditional, formal hierarchical structures is an inappropriate response to the current threat environment. The traditional, vertical model is ill equipped to deal with the vastly more complex issues and enemy strategies that the United States must face in the twenty-first century. Accountability must rest at the cognitively optimal level. If accountability rests with the local decision-maker, instead of passing all the way to the top, trust in subordinates can be re-established.

As Figure 6 shows, there is a direct relationship between environmental and task complexity and the organizational (and information handling) structure.

[107] Jansen. (2003). p. 13

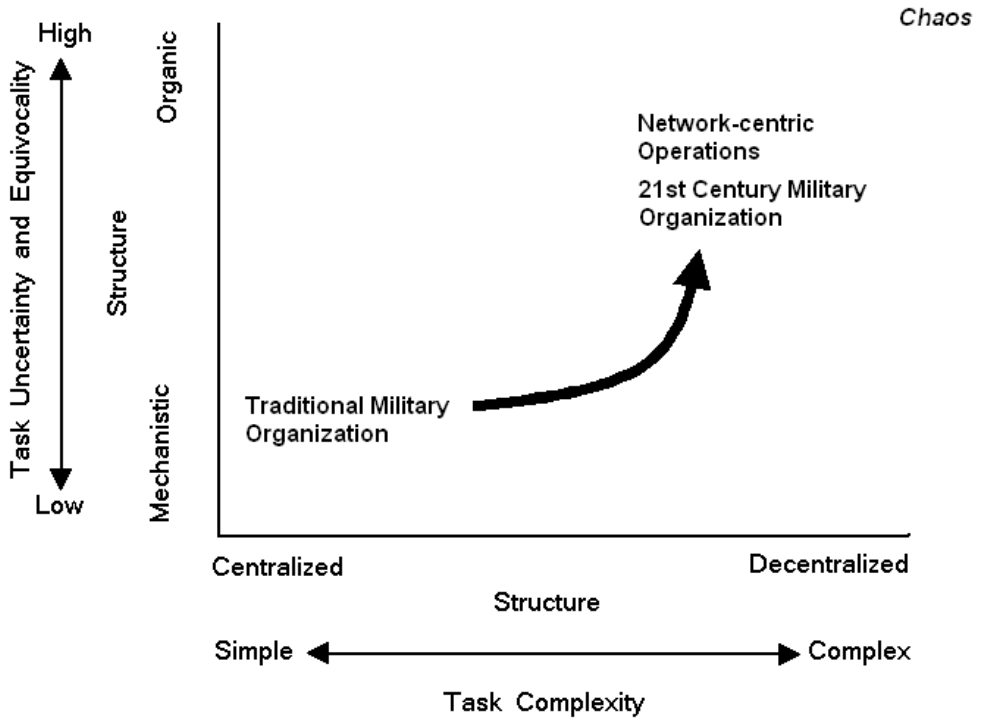


Figure 11. Shift in Organizational Configuration as Operational Military Organizations as Move into Network-Centric Operations
(Source: Jansen. 2003.)

As Carley, Lee and Krackhardt point out,

Individuals are more likely to develop effective leadership skills if they have high cognitive ability, prior experience, and extroversion. Individuals who have high cognitive ability and experience typically take on more tasks, are given more resources, and have more knowledge. Prior experience and extroversion often lead to a wider range of interaction partners. Stress typically occurs when cognitive load increases. Additionally, individuals are likely to emerge as leaders if they have high stress tolerance, have strong self-esteem and are open to new experiences. As such, they are likely to be willing to tell others what to do, shed tasks, give away resources, etc. Individuals with high cognitive loads are likely to be emergent leaders for a variety of reasons including they are most likely to tell others to do things (i.e., shed tasks) and most likely to be in a position of

> power in terms of what and whom they know. An agent is more likely to be an emergent leader and to direct the activity of the distributed network, even if only temporarily, if that agent is in a strong structural position in the social, knowledge and assignment networks. Overall cognitive load, not simply structural power, is key to tracking who is likely to be the emergent leader. Based on these considerations, we define the emergent leader as the individual with the highest cognitive load (the most people to talk to, the most information to process, the most tasks to do, the hardest tasks to do, the most people to negotiate with to get the job done, etc.[108]

Unfortunately, accountability at the top is an issue that has already "tipped," using Gladwell's terminology. Certain systems, like the use of the QWERTY keyboard layout and the two-party political system, become so ubiquitous that people resist changing them even when better alternatives are available; i.e., they have "tipped" or achieved a stable equilibrium. Small changes that make the alternatives more attractive to a critical mass of the total population can push tipped systems to favor the alternative, shifting the system to a different stable equilibrium. As it is, top leaders are the most easily identified and most easily targeted for public chastisement – witness calls for Defense secretary Rumsfeld's resignation in the aftermath of the Abu Ghurayb prison scandal. The way we think about accountability (the one at the top is accountable no matter what) is so widespread, it is simply accepted as *the* way to do things. It is what everyone is used to, and what everyone expects. Never mind the fact that often the man at the top has more information than he can competently handle (compared to what the commander on the ground may have.) Until a critical mass of the leadership cadre, both civil and military, formal and informal, accept and endorse cognitively optimal accountability levels as we have discussed, there is small hope of such cultural change.

2. Intelligence Information Communications Architecture

The Advanced Analysis Laboratory of the National Security Agency recently released a "Ten Most Wanted" list of capabilities for the intelligence community to develop. This study directly addresses three of them: Trust-building, Heterogeneous Collaboration, and Veiled Networks.

[108] Carley, et al. (2001). pp. 31-34

Trust-building: Much has been said and written about the insularity of intelligence agencies (and analysts) and about how we must overcome that parochialism by attacking rapidly-evolving, novel threats using *ad hoc* 'teams of strangers' recruited from throughout the Community…. When we literally have minutes to correlate and cross-inform analytic conclusions, we need methods other than 30-year associations for passing credentials and establishing *bona fides*.

Heterogeneous Collaboration: For the most part, current 'collaborative environments' reinforce this focus by requiring all participants to use a common suite of tools to portray and discuss the analytic domain. However, what if it were possible to introduce a collaboration interlocutor that was able to broker between an analytic issue as portrayed and manipulated in the domain of analyst A (say, a SIGINT analyst) and the same issue as dealt with in the domain of analyst B (an IMINTer, for example).

Veiled Networks: Today analysts concentrate on diagnosing and extracting intelligence from 'visible' networks—networks whose properties can be more or less directly observed. Analysts can thus figure out where to find bad guys in physical or logical communications networks, or how to infer bad guys' influences and intent from known properties of their social networks. We do not do so well, however, at inferring social arrangements from communications transactions, nor inferring the converse—anticipating communications that might confirm a social arrangement (e.g., a terrorist plot). Part of the problem lies in our ability to do the requisite collection and information extraction, an issue that has been around for decades. But the even deeper difficulty is that we have no efficient theory for attacking 'veiled networks'—networks whose properties are only seen dimly through the 'veil' of other networks.

Concerning trust-building and heterogeneous collaboration, I suggest adopting brokered file-sharing systems. Such systems can most rapidly meet the information needs of each node while ensuring trust and security. Web page-based systems like IntelLink represent a largely asynchronous, relatively labor-intensive mode of information dissemination, requiring regular updates and maintenance to sustain their utility. Their employment requires the widespread use of search engines, which may or may not always permit users to find the information they require within their given time constraints. Automating many of these processes and implementing appropriate *system-enforced* policies solve these problems. The intelligence computer communications networks should employ "bots" (automated, artificially intelligent software agents) to scan the information resident on the millions of intelligence systems and to retrieve the

information relevant to each unit's needs. These bots may reside on each unit's systems, or may reside on "broker" servers that employ bots on behalf of the requesting unit, as well as an automatically updated catalogue of available files. Each artificially intelligent bot would bear only the classification permission sets associated with the requesting unit, would have a memory of the kinds of information requested by its client unit, and could be programmed to suggest to its user information that the bot "thinks" might be useful and appropriate for the unit. Complex and time consuming procedures for requesting information from existing centralized broker agencies could be done away with. Message traffic routing could be accomplished in this way; with bots continuously updating the address lists based on clearance level, interest and need-to-know.

An effective automated implementation of mandatory and discretionary access control policies (MACs and DACs) within multi-level subject enabled broker servers can ensure both the security and integrity of data. DAC policies are commonly implemented in the Windows environment, and most systems administrators are familiar with them. They assign permissions to each user that control what he or she can access, and are set according to localized policies. MAC policies are not widely implemented within the Windows environment, appearing more commonly in UNIX systems. The best current models of MAC implementation are the Bell-LaPadula Security Model (BLP) and Biba Integrity Model. BLP prevents users at lower classification levels from accessing higher level materials (no read-up) and prevents higher level users from storing highly classified materials in lower level files, directories or systems (no write-down). Biba ensures the reliability of data on higher-level systems by enforcing a no read-down, no write-up policy. The two effectively lock the user into his or her classification and caveat permission set. The combination also can provide effective containment of malicious software.

In combination with MAC and DAC policies, auditing programs located on the broker servers, and the already widespread use of encryption in sensitive DoD networks, a link-encrypted p2p architecture would open the entire body of intelligence to any user cleared to access it. Such an implementation can reduce the cost associated with hardware purchase and replacement by minimizing the number of systems (and systems administrators) necessary to do intelligence work in a multiple level environ-

ment. By auditing and logging all transactions they handle, broker servers can provide a reliable and complete record of who had access to what information. Further implementation of a rating/reputation system (such as seen on E-pinions.com, E-bay, Kazaa, and numerous other online communities) can permit analysts to rate the reliability of the information and analysts they interact with, providing a self-policing system. With such automatic tracking of clearance level, expertise, and reputation, ad-hoc and heterogeneous collaboration teams can be assembled using chat forums and instant messaging in much the same way the enemies such as Al Qa'ida organize their operational elements, without the additional burden of researching each collaborator's *bona fides*.

To understand so-called "veiled networks" more adequately, a certain amount of *sociological intelligence* must be gathered about suspected members. Unfortunately, in viewing ourselves as a technological society in the reflection of our technological works, we have forgotten that we are a *human* society first. As anyone in the intelligence community can attest, technical intelligence (imagery, communications, signals, etc.) can never completely replace human intelligence. A map of an individual's social connections and the frequency of activations of these links are some of the metadata that provide clues about what sorts of communications to monitor for specific information. We need to see networks not in a mechanistic way, but as dynamic human systems, in the way that this thesis has expounded. Technologically mediated networks, and the ways in which they are used, reflect the social networks within which each person is embedded. Knowledge of the person, his or her position and roles, and his or her culture can facilitate predictive assessments, inferring social arrangements from communications transactions, or inferring the converse—anticipating communications that might confirm a social arrangement. In targeting a network, it is the metadata describing the links that must be analyzed and collected to effectively target networks.

3. Special Operations and Netwar

These techniques can work not just for intelligence organization, but also for our special operations organizations. SOF units organize regionally, meaning that they are expected to be experts in the political, religious, and cultural make-up of their region. A

brokered file-sharing architecture can ensure for them the same efficiency, speed, and security in their operations outlined above for the intelligence community. However, if they are to maximize the advantage that these powerful tools give them, they must have the distributed authority plan and conduct operations. As this thesis has asserted repeatedly, virtual organizations are localized phenomenon. That is, networks can be adaptable, responsive, and flexible only when they are locally controlled. Bin Ladin and his cohorts were brokers before they were leaders, and retain this function. Local operational cells, as revealed in Krebs' study have the authority to plan and conduct their own operations while relying on the rest of the network for support.

Unconventional warfare is exactly what Arquilla and Ronfeldt meant when they wrote about *netwar*. In destabilizing networks, it is the indirect approach, rather than the direct approach that is more effective. Software such as CONSTRUCT-O[109], as well as Valdis Krebs' network analysis software (InFlow) and influence-mapping programs like SIAM must be used in conjunction to perform multi-layered analysis of networks to define the "meta-matrix." This is a key factor in understanding social and technological network behavior. In fact, mapping and understanding the meta-matrix is the key to destabilizing networks. If the information about the *knowledge network* (who knows what), the *information network* (what ideas are related to what), the *assignment network* (who is doing what) and the *influence network* (who can do what) can be corrupted simultaneously, the entire network is likely to destabilize and collapse. Rather than focusing on taking out leaders, as most military strategists are wont to do, we should instead work on gaining access to and influence over the meta-information system, either through infiltration, recruitment, or, in the case of groups using computer-mediated communications technology, hacking with the purpose of performing computer network exploitation and computer network attack (the objective being to corrupt the meta-information, as opposed to performing denial of service attacks).

For example: We should target people like Stephenson's[110] "Gatekeepers" for collection/recruitment because they are likely to have the broadest tacit, if informal

[109] Ibid. p. 85

[110] Kleiner. (2003).

knowledge of the meta-networks. “Mavens” are hard to fool, but spoofing their identities and thereby borrowing their influence to spread would be effective, i.e., using their position in the influence network to affect the knowledge and information networks (recruiting them as agents would be even better.) “Salesmen” or Gatekeepers (being either persuasive personally or by network position) are also ideal candidates for spoofing or recruitment. It seems logical that the influence network should be used, rather than targeted, although the trade-off cost is that as misinformation is doled out, influence is likely to wane. Interestingly, “Pulsetakers” or “Connectors” tend not to figure strategically in attacking strong-tie networks, except as easily replaceable leaders, because they tend to trade in primarily weak ties. Strategy must therefore be adapted *to the primary mode of connectedness* of the targeted network.

Such courses of action are intelligence-intensive, and rely on both clandestine technical collection and human intelligence (HUMINT). Communications intelligence (COMINT) should be collected not just on message content, but also on meta-data for analysis: DNS/IP addresses, e-mail addresses, number of links per node, who links to whom and why. Once the meta-information network is mapped and modeled (exploitation), an attack would consist of creating misdirected flows through deceptive identity-performance and disinformation. The object is to ensure that no one in the network is able to link ideas, link to knowledgeable members, or to operational members. By doing so, trust is globally diminished (meta-information is often taken for granted, and is often the unacknowledged basis for trust).

An understanding of the meta-network, including especially information diffusion patterns and rates, to identify critical flows in each metalayer network (knowledge, information, influence and assignment networks) can be applied constructively as well. In the cases of Afghanistan and Iraq, comprehensive models of the social meta-networks are vital; such information can be used effectively to integrate and coordinate information, influence, and unconventional warfare operations when conducting both counter-

insurgency operations (disrupting bad networks) and nation-building operations (constructing good networks)[111].

The case study of online pedophiles provides a cautionary note. Clandestine purposes can lead to a crippling preoccupation with security. While the rise of the Internet offered new forums and techniques for pederasts to indulge their individual compulsions, it effectively destroyed what limited semblance of organization and sense of community they might have had. Their online activities are now highly individualized; effectively marginalizing them as a social or political force, and even preventing them from seeking the help they need to escape the downward spiral of their illness.

4. Recruiting Netwarriors

Let us revisit the questions posed by the USAF Institute for National Security Studies (INSS):

- Is there any effective way to recruit the "Info Operators" necessary to maintain superiority in the various aspects of information warfare operations?
- Are we currently using effective techniques for recruiting airmen, soldiers, and sailors who are better suited to information operations?
- Do entrance tests (enlisted or officer) adequately measure the aptitude and skills needed for IW?
- Should recruiting of IW be tailored differently than other military fields?

Traditional intelligence tests may provide a good starting point for locating these people, as well as academic performance. However, such tests are only suggestive, and cannot provide definitive evidence of network aptitude. Moreover, network capital is acquired, rather than inherent, and is based in no small measure on sociability.

Netwarriors then, must be intelligent, educated, and also highly social individuals. The popular idea of Infowarriors as groups of highly intelligent, technically skilled but asocial "nerds" is in error. Temperament indicators, such as the Myers-Briggs personality test, in conjunction with cognitive assessments, and academic achievement and per-

[111] I say nation building as opposed to state building because the forms of the state should derive from and support a strong integrative societal network with a concurrent shared identity; i.e., the nation must pre-exist the state.

formance may be useful in identifying potential Information Operators. Finding highly social individuals is important, but developing and maintaining sociability is equally vital. The problem is that the conventional mindset sees CMCT as merely a tool, and separates the social aspects of the technology from its more technical aspects. The absence of widespread use of chat or instant messaging applications on military intranets is evidence of this. Encouraging social uses of CMCT can foster the familiarity with social networking so critical to network capital. Strong face-to-face ties are not as necessary as an aggregate sense of mission and open communications are to developing group identity.

Highly social people tend also to be highly empathetic. This empathy may enable them to more effectively prosecute PSYOP and influence campaigns – especially if armed with the social intelligence/metadata described above.

Current entrance tests for all military personnel, Officers and Enlisted, include the Armed Services Vocational Aptitude Battery (ASVAB) and the Armed Forces Qualifying Test (AFQT) test only a rather limited number of areas. The ASVAB, for example, tests word knowledge, paragraph comprehension, arithmetic reasoning, mathematics knowledge, general science, auto and shop information, mechanical comprehension, electronics information, numerical operations, coding speed and assembling objects. The AFQT comprises only four sections of the ASVAB (Word Knowledge, Paragraph Comprehension, Arithmetic Reasoning, and Mathematics Knowledge.) Test results determine only whether one qualifies for military service, and if so, for what jobs one qualifies. For officers, scores from standardized college entrance exams (SAT, ACT, and GRE) are considered as well.

High scores (Category I and Category II only) in all areas of the ASVAB should be requisite for netwarriors; however, the AVAB should incorporate tests of individuals' social aptitude as well, such as an abbreviated Myers-Briggs profile that could discern extroverts from introverts. Moreover, current ASVAB scores are based on a 1980 DoD sponsored study that surveyed the vocational aptitude of young people. Fortunately,

the new standards (based on a 1997 survey) are to be released in July this year.[112] However, the new study still does not measure the social aptitude of applicants.

D. AREAS FOR FURTHER RESEARCH

As identified in various sections throughout this thesis, the following topics present challenging, but necessary areas for pure and applied research into cybersociology:

- Case Studies of Open/Illegitimate Communities and Closed/Legitimate Communities (Communities of Practice)
- Cultural Embeddedness of Individual Action and Computer Networking
- Case Studies of Al Qa'ida Members' Online Behavior
- Social Networking Behavior among Online Pedophiles
- Social Warfare Among *EverQuest* Guilds
- Demographic Analysis of Various Online Communities
- Implementation of a Distributed P2P Architecture Within DoD Intelligence Networks
- Developing Standards of Social Networking Ability for Inclusion in Armed Forces Recruiting Tests (ASVAB/AFQT)
- Developing Methods of Detecting and/or Cultivating Social Networking Ability in Military Personnel

[112] http://www.defenselink.mil/releases/2004/nr20040206-0332.html

LIST OF REFERENCES

Aihoshi, R. (27 Sep 2000). Brad McQuaid Interview. San Francisco, CA: IGN Entertainment, Inc. Retrieved 5 May 2004 from: http://rpgvaultarchive.ign.com/features/interviews/bmcquaid_a.shtml

Alsayyad, N. and Castells, M. Eds. (2002). *Muslim Europe or Euro-Islam: Politics, Culture, and Citizenship in the Age of Globalization*. Lanham, MD: Lexington Books.

Anderson, B. (1991). *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. New York: Verso.

Arquilla, J. and Ronfeldt, D.
(1997). *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA. RAND.
(2001). *Networks and Netwars.* Santa Monica, CA. RAND.

Burkhart, G. and Older, S. (2003) *The Information Revolution in the Middle East and North Africa*. Santa Monica, CA: RAND. Retrieved 9 December 2003 from: www.rand.org/publications/MR/MR1653/MR1653.pdf

Carley, C., Lee, J. and Krackhardt, D. (2002). Destabilizing Networks. *Connections*. Vol. 24, No. 3. INSNA

Castells, M. (2000). *The Network Society*. Oxford, UK: Blackwell Publishers.

Choi, H. (2003). Ethnic Clustering in Blogging Communities. Retrieved 6 April 2004 from: http://www.students.haverford.edu/hchoi/final%20project.htm

Cooper, Al. (2002). *Sex & the Internet: A Guidebook for Clinicians*. New York: Brunner-Routledge

Cooper, A., Scherer, C., Boies, S. and Gordon, B. (1999). Sexuality on the Internet: From *Sexual Exploration to Pathological Expression*. Edit Proof. Courtesy Dr. Al Cooper, Clinical Director, San Jose Marital and Sexuality Center. Santa Clara, CA

Csapo, N. (August 2002). Certification of Computer Literacy. *The Journal*. Vol. 30, No. 1. Retrieved 4 December 2003 from:
http://www.thejournal.com/magazine/vault/A4117.cfm

CSTIW.
(2000). *Escalatory Dynamics in Sub-State Conflict: Cyberterrorism and Mass Casualties*. Final report on a conference held May 15-17, 200 at the University Pantheon-Assas (Paris II). p. 16. Courtesy Dr. Dorothy Denning, Naval Postgraduate School.

Denning, D.
(1999). *Information Warfare and Security*. New York: ACM Press/Addison-Wesley
(May 17, 2004) Terrorism and Information Operations. Unpublished article. Monterey, CA: Naval Postgraduate School. Courtesy Dr. Denning.

Eedle, P. (July 17 2002). Terrorism.Com. *The Guardian*. London. Retrieved 10 Dec 2003 from:
http://www.guardian.co.uk/afghanistan/comment/story/0,11447,756638,00.html

Fandy, M. (February 2001). *Saudi Arabia and the Politics of Dissent*. London: Palgrave-MacMillan.

Garreau, J. (September 17, 2001). Disconnecting the Dots. *The Washington Post*. p. C01

Gause, F. (1994). *Oil Monarchies: Domestic and Security Challenges in the Arab Gulf*. Interuniversity Consortium for Arab Studies, Montreal. Retrieved 3 December 2003 from: http://www.arts.mcgill.ca/programs/icas/gause/chapter2.html.

Gladwell, M. (2002). *The Tipping Point: How Little Things Can Make a Big Difference*. New York: Little, Brown and Company.

Glatzer, B. (2002). The Pashtun Tribal System. In Pfeffer and Behera (Eds.): *Concepts of Tribal Society. Contemporary Society: Tribal Studies, Vol 5*. New Delhi: Concept Publishers

Granovetter, M.
(1973). The Strength of Weak Ties. *American Journal of Sociology*. Volume 78. pp.1360-80
(1983) The Strength of Weak Ties: A Network Theory Revisited. *Sociological Theory*. Volume 1. pp. 201-233.
(1985). Economic Action and Social Structure: The Problem of Embeddedness, *American Journal of Sociology*. Volume 91. pp. 481-510.

Guralnik, D. ed. (1984). *Webster's New World Dictionary of the American Language*. New York: Warner Books.

Hamman, R.
(1996) Cyborgasms: Cybersex amongst Multiple-Selves and Cyborgs in the Narrow-Bandwidth Space of America Online Chat Rooms. Retrieved 15 May 2004 from: http://www.socio.demon.co.uk/Cyborgasms.html
(1999). Computer Networks Linking Network Communities: A Study of the Effects of Computer Network Use upon Pre-existing Communities. *Cyberociology Magazine*. Retrieved 25 May 2004 from: http://www.socio.demon.co.uk/mphil/short.html

Hayot, E. and Wesp, E. (2004) Reading Game/Text: *EverQuest*, Alienation, and Digital Communities. Johns Hopkins University Press. Retrieved 9 May 2004 from: http://www.iath.virginia.edu/pmc/current.issue/14.2hayot_wesp.html

Hine, C. (2000). *Virtual Ethnography*. Sage Publications: Thousand Oaks, CA.

Homer-Dixon, T. (Jan-Feb 2002). The Rise of Complex Terrorism. *Foreign Policy Magazine*. Retrieved 1 December 2003 from: http://www.foreignpolicy.com/issue_janfeb_2002/homer-dixon.html.

Hudson, R. et al. (September 1999). *The Sociology and Psychology of Terrorism: Who Becomes A Terrorist and Why*. Washington, D.C.: Federal Research Division, Library of Congress. Retrieved September 21 2003 from: http://www.fas.org/irp/threat/frd.html

Innocent Images Operation Candyman Phase I. (March 18, 2001). FBI National Press Office. Washington, DC. Retrieved February 17 from: http://www.fbi.gov/pressrel/candyman/candymanhome.htm

Jakobsson, M. and Tyler, T. (2003). The Sopranos Meets EverQuest: Social Networking in Massively Multiplayer Online Games. *MelborneDAC2003*, Melbourne, Australia. Retrieved January 16, 2004 from: http://hypertext.rmit.edu.au/dac/papers/Jakobsson.pdf

Jansen, E. (2003) *The Officers of the Future: Thinking Through the Revolution*. Unpublished Working Paper. Monterey, CA. Naval Postgraduate School.

Joint Chiefs of Staff (9 Oct 1998). *Joint Publication 3-13*, *Joint Doctrine for Information Operations.*

Kadushin, C. (May 2000). *A Short Introduction to Social Networks: A Non-Technical Elementary Primer*. Retrieved 14 August 2003 from: http://construct.haifa.ac.il/~cerpe/papers/kadushin.html.

Kalathil, S. and Boas, T. (2003). *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Washington, D.C.: Carnegie Endowment for International Peace/Brookings Institution Press.

Kali, R. (January 2003). *Social Embeddedness and Economic Governance: A Small World Approach*. University of Arkansas. Retrieved 5 December 2003 from: http://www.cramton.umd.edu/workshop/ papers/kali-small-world.pdf

Kleinberg, J. (1999). *The Small-World Phenomenon: An Algorithmic Perspective*. Cornell University. Retrieved 5 December 2003 from: http://www.cs.cornell.edu/home/kleinber/swn.d/swn.html.

Kleiner, A. (2003). Karen Stephenson's Quantum Theory of Trust. *strategy+business*. Retrieved 3 Mar 2004 from: http://www.strategy-business.com/press/prnt/?ptag-ps=&art=9056282&pg=0&format=print

Knapp, M. (2003). *Al-Qaida's Use of the Mass Media in Infowar/Netwar*. Unclassified briefing prepared for the National Ground Intelligence Center. (Courtesy Michael Knapp.)

Koontz, L. (September 9, 2003). *File Sharing Programs: Users of Peer-to-Peer Networks Can Readily Access Child Pornography*. Government Accounting Office Report GAO-03-1115T. GAO: Washington, DC. Retrieved 26 March 2004 from GAO Web site: http://frwebgate.access.gpo.gov/cgi-bin/multidb.cgi

Krebs, V. (2002). *Mapping Networks of Terrorist Cells*. Retrieved 28 November 2003 from: http://www.orgnet.com.

Kurose, J. and Ross, K. (2003). *Computer Networking: A Top-Down Approach Featuring the Internet*. Second Edition. Pearson Education, Inc.

Lebo, H. and Wolpert, S. (14 Jan 2004). *First Release of Findings from the UCLA World Internet Project Shows Significant 'Digital Gender Gap' in Many Countries*. *UCLA News*. Retrieved 14 Jan 2004 from: http://www.uclanews.ucla.edu.

Leiblum, S. (1997). Sex and the Net: Clinical Implications. *Journal of Sex Education and Therapy*, 22 (1), 21-28.

Lin, Nan. (2001.) *Social Capital: A Theory of Social Structure and Action*. New York: Cambridge University Press.

Ludlow, P. (ed.) *Crypto Anarchy, Cyberstates, and Pirate Utopias*. Cambridge, MA: The M.I.T. Press.

McLaughlin, J. (January 2000). *Cyber Child-Sex Offender Typology*. Retrieved 5 May 2004 from: http://www.ci.keene.nh.us/police/Typology.html.

Milward, H. and Raab, J. (October 2002). *Dark Networks: The Structure, Operation, and Performance of International Drug, Terror, and Arms Trafficking Networks*. Retrieved 4 December 2003 from: www.iigov.org/workshop/pdf/Milward_and_Raab.pdf

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M. & Gagnon, G. (1999). *Cyberterror: Prospects and Implications*. White Paper prepared for the Defense Intelligence Agency, Office for Counterterrorism Analysis. Monterey, CA: CSTIW.

Preece, J. (2000). *Online Communities: Designing Usability, Supporting Sociability*. New York: John Wiley and Sons.

Preece, J., Maloney-Krichmar, D. & Abras, C (2003). History of the Emergence of Online Communities. In B. Wellman (Ed.), *Encyclopedia of Community*. Berkshire Publishing Group, Sage. Retrieved 6 April 2004 from: http://www.ifsm.umbc.edu/~preece/paper/6%20Final%20Enc%20preece%20et%20al.pdf.

Putnam, R. (December 1995) Tuning in, Tuning out: The Strange Disappearance of Social Capital in America. *Political Science and Politics*.

New Study Shatters Internet 'Geek' Image. (14 January 2004). *Reuters*. Retrieved 14 Jan 2004 from: http://www.cnn.com/

Rheingold, H. (2002). *Smart Mobs: The Next Social Revolution*. New York: Perseus Publishing.

Roach, S. (June 28, 2000). *Global: The Digital Divide*. Morgan Stanley & Co. Incorporated and Dean Witter Reynolds Inc. Retrieved 4 December 2003 from: http://www.morganstanley.com/GEFdata/digests/20000628-wed.html

Sandberg, O. and Wiley, B. (Spring 2002). Protecting Free Expression Online with Freenet. *IEEE Internet Computing*. Retrieved 3 March 2004 from: http://freenet.sourceforge.net/papers/freenet-ieee.pdf

Smith, A. (Spring 2000). *From the Feel of the Page or the Touch of a Button: Envisioning the Role of Digital Technology in the English and Language Arts Classroom*. Retrieved 3 December 2003 from: http://www.msu.edu/~smitha62/computer.htm

Stone, A. (1991). *Will the Real Body Please Stand Up?* Retrieved 6 April 2004 from: http://www.rochester.edu/College/FS/Publications/StoneBody.html

Svensson, J. and Bannister, F. (June 2004). Pirates, Sharks and Moral Crusaders: Social control in Peer–to–Peer Networks. *First Monday: Peer Reviewed Journal on the Internet*. Issue 9. Retrieved 8 June 2004 from http://firstmonday.org/issues/issue9_6/svensson/

Sztompka, P. (1999). *Trust: A Sociological Theory*. New York: Cambridge University Press.

Thomas, T. (Spring, 2003). Al Qaeda and the Internet: The Danger of Cyberplanning. *Parameters*. 33 (1). Retrieved 15 November from: http://carlisle-www.army.mil/usawc/parameters/03spring/thomas.pdf

Verton, D. (November 18 2002). Bin Laden Cohort Warns of Cyberattacks. *Computer-world Online Magazine*. Retrieved 5 December 2003 from: http://www.intellnet.org/news/2002/11/18/13650-1.asp

Yamagishi, T. (2001). Trust as Social Intelligence. In K. Cook (Ed.), *Trust in Society*. New York: Russell Sage Foundation.

Young, K. (1997). *Internet Addiction: What Makes Computer-Mediated Communication Habit Forming?* Paper presented at the 105th Annual convention of the American Psychological Association, Chicago, IL. Courtesy Dr. Al Cooper, Clinical Director, San Jose Marital and Sexuality Center. Santa Clara, CA

Web-Only Material:

http://devdata.worldbank.org/data-query/ (Retrieved 5 December 2003)

http://eqlive.station.sony.com

www.internetworldstats.com

http://www.emergency.com/2003/Khalid_Shaikh_Mohammedprofile.htm (Retrieved 5 December 2003)

http://www.nua.com/surveys/how_many_online/index.html (Retrieved 5 December 2003)

http://www.pbs.org/wgbh/pages/frontline/shows/network/personal/ (Retrieved 5 December 2003)

http://www.freespirits.org (Retrieved 18 April 2004)

http://www.prevent-abuse-now.com/pedoweb2.htm (Retrieved 18 April 2004)

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Dorothy Denning
   Department of Defense Analysis
   Naval Postgraduate School
   Monterey, California

4. Dr. John Arquilla
   Department of Defense Analysis
   Naval Postgraduate School
   Monterey, California

5. Dr. Gordon McCormick
   Department of Defense Analysis
   Naval Postgraduate School
   Monterey, California

6. Jennifer Duncan
   Department of Defense Analysis
   Naval Postgraduate School
   Monterey, California